

UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA
STRENGTH and WISDOM

NATO CYBERSPACE CAPABILITY: A STRATEGIC AND OPERATIONAL EVOLUTION

Jeffrey L. Caton

U.S. ARMY WAR COLLEGE
SSI
STRATEGIC STUDIES INSTITUTE

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.

The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.

The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE



The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

Strategic Studies Institute
and
U.S. Army War College Press

NATO CYBERSPACE CAPABILITY: A STRATEGIC AND OPERATIONAL EVOLUTION

Jeffrey L. Caton

June 2016

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5010.

*****

This manuscript was funded by the U.S. Army War College External Research Associates Program. Information on this program is available on our website, *www.StrategicStudiesInstitute.army.mil*, at the Opportunities tab.

*****

*****

The Strategic Studies Institute and U.S. Army War College Press publishes a monthly email newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on the SSI website at *www.StrategicStudiesInstitute.army.mil/newsletter.*

ISBN 1-58487-728-6

FOREWORD

Several years ago, as the primary focus of U.S. military strategy shifted to the western Pacific region, many respected authorities began to question the relevance of the North Atlantic Treaty Organization (NATO) in modern world events. More recent events, such as the Russian Federation's annexation of Crimea, have given policy makers pause to question the wisdom of anticipated force cuts in Europe. Amidst this turmoil, the staffs of U.S. European Command and U.S. Army Europe have been establishing and refining their capabilities to conduct military operations in and through the cyberspace realm.

If indeed the decision is made to pursue military action in cyberspace, what capabilities are available within NATO forces to accomplish such activities? What organization, doctrine, and methods would guide operators who perform such actions? In this monograph, Mr. Jeffrey Caton explores these questions within the broader context of the continued evolution of the NATO Alliance. He argues that the overall state of cyberspace activities within NATO appears to be sound and that continued resourcing for, and pursuit of, improved cyberspace capabilities by U.S. military forces in Europe will help to ensure the steady progress of NATO cyberspace endeavors.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
U.S. Army War College Press

ABOUT THE AUTHOR

JEFFREY CATON is President of Kepler Strategies LLC, Carlisle, Pennsylvania, a veteran-owned small business specializing in national security, cyberspace theory, and aerospace technology. He is also an Intermittent Professor of Program Management with the Defense Acquisition University. From 2007-2012, Mr. Caton served on the U.S. Army War College faculty, including as an associate professor of cyberspace operations and Defense Transformation Chair. Over the past 7 years, he has presented lectures on cyberspace and space issues related to international security in the United States, Sweden, the United Kingdom, Estonia, Kazakhstan, and the Czech Republic supporting programs such as the Partnership for Peace Consortium and the NATO Cooperative Cyber Defence Center of Excellence. His current work includes research on cyberspace and autonomous weapons issues as part of the External Research Associates Program of the Strategic Studies Institute. Mr. Caton is also a member of the Editorial Board for *Parameters* magazine.

He served 28 years in the U.S. Air Force, working in engineering, space operations, joint operations, and foreign military sales, including command at the squadron and group level. Mr. Caton holds a bachelor's degree in chemical engineering from the University of Virginia, a master's degree in aeronautical engineering from the Air Force Institute of Technology, and a master's degree in strategic studies from the Air War College.

SUMMARY

The development of cyberspace defense capabilities for the North Atlantic Treaty Organization (NATO) has been making steady progress since its formal introduction at the North Atlantic Council Prague Summit in 2002. Bolstered by numerous cyber attacks such as those in Estonia in 2007, Alliance priorities were formalized in subsequent NATO cyber defense policies that were adopted in 2008, 2011, and 2014. This monograph examines the past and current state of NATO's cyberspace defense efforts by assessing the appropriateness and sufficiency of them to address anticipated threats to member countries, including the United States. This analysis focuses on the recent history of NATO's cyberspace defense efforts and how changes in NATO's strategy and policy writ large embrace the emerging nature of cyberspace for military forces, as well as other elements of power. In general, the topics presented herein are well documented in many sources. Thus, this monograph serves as a primer for current and future operations and provides senior policymakers, decision-makers, military leaders, and their respective staffs with an overall appreciation of existing capabilities as well as the challenges, opportunities, and risks associated with cyberspace-related operations in the NATO context. The scope of this discussion is limited to unclassified and open source information; any classified discussion must occur within another venue.

This monograph has three main sections:

- NATO Cyberspace Capability: Strategy and Policy. This section examines the evolution of the strategic foundations of NATO cyber activities, policies, and governance as they evolved over the past 13 years. It analyzes the content of

the summit meetings of the NATO North Atlantic Council for material related to cyber defense. It also summarizes the evolution of NATO formal cyber defense policy and governance since 2002.

- NATO Cyberspace Capability: Military Focus. NATO cyber defense mission areas include NATO network protection, shared situational awareness in cyberspace, critical infrastructure protection (CIP), counter-terrorism, support to member country cyber capability development, and response to crises related to cyberspace. This section explores these mission areas by examining the operations and planning, doctrine and methods, and training and exercises related to NATO military cyberspace activities.
- Key Issues for Current Policy. The new Enhanced Cyber Defence Policy affirms the role that NATO cyber defense contributes to the mission of collective defense and embraces the notion that a cyber attack may lead to the invocation of Article 5 actions for the Alliance. Against this backdrop, this section examines the related issues of offensive cyberspace, deterrence in and through cyberspace, legal considerations, and cooperation with the European Union.

This monograph concludes with a summary of the main findings from the discussion of NATO cyberspace capabilities and a brief examination of the implications for Department of Defense and Army forces in Europe. Please note that the European spelling of some words (e.g., defence) may be used throughout this monograph to ensure the accuracy of NATO organizational and operational titles.

ACRONYMS

ACO	Allied Command Operations
ACT	Allied Command Transformation
AJP	Allied Joint Publication
C4	Command, Control, Communications and Computer
CCD COE	Cooperative Cyber Defence Center of Excellence
CDC	Cyber Defence Committee
CDMA	Cyber Defence Management Authority
CDMB	Cyber Defence Management Board
CDSA	Cyber Defence Situational Awareness
CERT	Computer Emergency Response Team
CFI	Connected Forces Initiative
CICOA	Cyber Implications for Combined Operational Access
CIICS	Cyber Information and Incident Coordination System
CIIP	critical information infrastructure protection
CIP	critical infrastructure protection
CIS	communication and information system
CJOS COE	Combined Joint Operations from the Sea Centre of Excellence
COE-DAT	Centre of Excellence Defence Against Terrorism
COPD	Comprehensive Operations Planning Directive
CPAL	Cyber Prioritized Asset List
CRAM	Cyber Risk Assessment Matrix
CSAT	Cyber Security Assessment Team

DMCCI	Distributed Multi-sensor Collection and Correlation Infrastructure
EDA	European Defence Agency
ENISA	European Network and Information Security Agency
EU	European Union
FM	Field Manual
FOC	full operational capability
GSP	Government Security Program
JFCBS	Joint Force Commands in Brunssum
JFCNP	Joint Force Commands in Naples
JP	Joint Publication
MCDC	Multinational Capability Development Campaign
MDCO	Multinational Defensive Cyber Operations
MISP	Malware Information Sharing Platform
MN CD E&T	Multinational Cyber Defence Education and Training
MN CD2	Multinational Cyber Defence Capability Development
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization
NCI Agency	NATO Communications and Information Agency
NCIRC	NATO Computer Incident Response Capability.
NCISS	NATO Communications and Information Systems School.
NCS	NATO Command Structure
NDPP	NATO Defence Planning Process
NICP	NATO Industry Cyber Partnership
OCO	offensive cyberspace operations
RRT	rapid reaction team

SACEUR	Supreme Allied Commander Europe
SHAPE	Supreme Headquarters Allied Powers Europe
TRJE15	Trident Juncture 2015 Exercise
USAREUR	U.S. Army Europe
USEUCOM	U.S. European Command
WARP	Warning Advice and Reporting Points

NATO CYBERSPACE CAPABILITY: A STRATEGIC AND OPERATIONAL EVOLUTION

INTRODUCTION

The development of cyberspace defense capabilities for the North Atlantic Treaty Organization (NATO) has been making steady progress since its formal introduction at the North Atlantic Council Prague Summit in 2002. Bolstered by numerous cyber attacks such as those in Estonia in 2007, Alliance priorities were formalized in subsequent NATO cyber policies that were adopted in 2008, 2011, and 2014. This monograph examines the past and current state of NATO's cyberspace defense efforts by assessing the appropriateness and sufficiency of them to address anticipated threats to member countries, including the United States. This analysis focuses on the recent history of NATO's cyberspace defense efforts, and how changes in NATO's strategy and policy writ large embrace the emerging nature of cyberspace for military forces as well as other elements of power. In general, the topics presented herein are well documented in many sources. Thus this monograph serves as a primer for current and future operations to provide senior policymakers, decision-makers, military leaders, and their respective staffs with an overall appreciation of existing capabilities as well as the challenges, opportunities, and risks associated with cyberspace-related operations in the NATO context.

NATO CYBERSPACE CAPABILITY: STRATEGY AND POLICY

The founding principles of NATO were the collective defense, crisis management, and cooperative security amongst its member countries. Conceived in a Cold War environment, the Alliance has endured strategic changes through major conflicts and the global power shifts that eventually led to the fall of the Warsaw Pact. After a brief period where some pundits questioned its relevancy, NATO has experienced a renaissance of its core security functions with the adoption of a new Strategic Concept in 2010. This section examines the recent evolution of the strategic foundations of NATO cyber activities, policies, and governance as they evolved over the past 13 years.

Cyberspace Addressed in Major Accords.

The 2002 NATO North Atlantic Council (NAC) Summit in Prague, Czech Republic marked the entry of cyber defense as a significant issue worthy of the collective attention of the Alliance.[1] Leaders at the summit directed the creation of a technical NATO cyber defense program that included the establishment of the NATO Computer Incident Response Capability (NCIRC).[2]

While work on cyber defense progressed, there was no mention of it in a NAC summit again until the 2006 meeting in Riga, Latvia. Table 1 summarizes the key strategic-level content from NATO summit meetings held over the past decade (see the Appendix for the verbatim excerpts of cyber-related content from these meetings).

NATO North Atlantic Council Summit Meeting	Key Strategic Cyberspace-Related Issues in Summit Declaration
Riga, Latvia November 29, 2006	• Endorsed work to develop a NATO Network Enabled Capability to share information in Alliance operations and improve protection against cyber attack.[3]
Bucharest, Hungary April 3, 2008	• Adopted an initial Policy on Cyber Defense and development of supporting structures and authorities to implement it.[4]
Strasbourg-Kehl, France/Germany April 2-3, 2009	• Established a NATO Cyber Defence Management Authority (CDMA). • Improved the existing Computer Incident Response Capability. • Activated the Cooperative Cyber Defence Centre of Excellence (CCD COE) in Estonia.[5]
Lisbon, Portugal November 20, 2010	• Called for an updated NATO in-depth cyber defense policy by June 2011 as well as a supporting action plan. • Accelerated goal of NATO Computer Incident Response Capability (NCIRC) to Full Operational Capability (FOC) by 2012. • Called for all NATO bodies to be under centralized cyber protection. • Use NATO's defense planning processes to develop Allies' cyber defense capabilities and improve interoperability. • Work closely with other actors, such as the United Nations (UN) and the European Union (EU).[6]

Table 1. Key Cyber Issues at Recent NATO North Atlantic Council Summit Meetings.

NATO North Atlantic Council Summit Meeting	Key Strategic Cyberspace-Related Issues in Summit Declaration
Chicago, Illinois, USA May 20, 2012	• Confirmed adoption of a new Cyber Defence Concept, Policy, and Action Plan. • Reiterated efforts to improve NATO capabilities and planning to address cyber attacks by continuing to pursue centralized cyber protection of NATO bodies; integrate cyber defense into Alliance structures and procedures and strengthen Alliance collaboration and interoperability.[7]
Newport, Wales, UK September 5, 2014	• Endorsed an Enhanced Cyber Defence Policy. • Reaffirmed ongoing efforts to improve NATO capabilities and planning to address cyber attacks through new initiatives with industry; with cyber defense education, training, and exercise activities; and with a cyber range capability.[8]

Table 1. Key Cyber Issues at Recent NATO North Atlantic Council Summit Meetings. (cont.)

The 2009 Annual Session of the NATO Parliamentary Assembly included a report, "NATO and Cyber Defence," that provided an in-depth review of the key issues faced by the Alliance in the cyberspace realm. The report's conclusion characterized the urgent need for NATO cyber defense:

> All indications signal that cyber attacks are now one of the most serious asymmetric threats faced by the Alliance and its member states, along with terrorism and nuclear proliferation. The open nature of the Internet makes preventing cyber attacks difficult; effective

> international cooperation will be critical to addressing this problem in the years to come. As the world's premier collective defence entity, NATO has a responsibility to take adequate measures to protect itself from such threats, as well as having a potentially significant role to play in contributing to the cyber defence of its Members, both through deterrence and by coordinating common cyber security measures. NATO's new strategic concept should reflect this important new element of Alliance activity. National parliamentarians have an important role to play in hastening the implementation of NATO's cyber defence policy, as well as ensuring that cyber security measures are responsibly put in place and exercised at the domestic level.[9]

A significant outcome of the 2010 Lisbon Summit was the adoption of a new NATO Strategic Concept: "Active Engagement, Modern Defence."[10] This official document describes NATO's enduring purpose, fundamental security tasks, and anticipated security environment. It also provides guidance on how military forces should adapt to implement the new concept. There have been only six previous Strategic Concepts, the first four of which were classified documents that reflected the evolution of NATO throughout the Cold War and addressed issues such as the doctrines of massive retaliation and flexible response for nuclear weapons. Strategic Concepts in 1991 and 1999 addressed the emerging challenges of a post-Cold War geopolitical environment.[11]

"Active Engagement, Modern Defence" is focused on three essential core tasks: collective defense, crisis management, and cooperative security.[12] Its section describing "The Security Environment" includes a paragraph that states, "cyber attacks are becoming more frequent, more organized and more costly in damage" to governments and industries in the

alliance. It also notes that such attacks may not only come from foreign militaries, but also from "organized criminals, terrorists and/or extremist groups."[13] The Strategic Concept's section on "Defence and Deterrence" outlines the scope of military capabilities required by NATO to cope with challenges such as nuclear operations, ballistic missile defense, expeditionary operations, counter-terrorism measures, and energy security. It also explicitly mentions the broad areas of capability required to confront cyber attacks:

> We will ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of our populations. Therefore, we will…develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations.[14]

Cyber Policy and Governance.

An initial NATO Cyber Defence Policy was adopted at the 2008 NATO NAC Summit in Bucharest. The policy was then updated after the 2010 Lisbon Summit and again after the 2014 Wales Summit. Table 2 summarizes the key tenets of each of these policies. The 2008 version provided some of the foundational elements for future policies and began the process of centralizing NATO cyber efforts through institutions such as the Cyber Defence Management Authority (CDMA). The CDMA mission was "to initiate and coordinate cyber defenses, review capabilities, and conduct appropriate risk management."[15]

The 2011 NATO Cyber Defence Policy followed the adoption of the new NATO Strategic Concept and thus focused on methods to further NATO's collective ability "to prevent, detect, defend against and recover from cyber-attacks."[16] It also established a cyber defense governance with a hierarchy that flowed from the NAC to the Defence Policy and Planning Committee in Reinforced Format, then to the NATO Cyber Defence Management Board (CDMB), and finally to the NCIRC.[17]

Year	Key Tenets of NATO Cyber Policy
2008	• Emphasize protection of key information systems. • Share best practices for cyber defence. • Develop capability to assist Allied nations, upon request, to counter cyber attack. • Develop NATO's cyber defence capabilities. • Strengthen linkage between NATO and national authorities.[18]
2011	• Integrate cyber defence considerations into NATO structures and planning processes in order to perform NATO's core tasks of collective defence and crisis management. • Focus on prevention, resilience, and defence of critical cyber assets to NATO and Allies. • Develop robust cyber defence capabilities and centralize protection of NATO's own networks. • Develop minimum requirements for cyber defence of national networks critical to NATO's core tasks. • Provide assistance to the Allies to achieve a minimum level of cyber defence and reduce vulnerabilities of national critical infrastructures. • Engage with partners, international organizations, the private sector and academia.[19]

Table 2. Key Tenets of NATO Cyber Defence Policy Versions.

Year	Key Tenets of NATO Cyber Policy
2014	• Reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. • Recalls that the fundamental cyber defense responsibility of NATO is to defend its own networks. • Emphasizes responsibility of Allies to develop relevant capabilities for protection of their national networks. • Recognizes that international law applies in cyberspace. • Affirms that cyber defence is part of NATO's core task of collective defense under Article 5.[20]

Table 2. Key Tenets of NATO Cyber Defence Policy Versions. (cont.)

The 2014 NATO Enhanced Cyber Defence Policy refines cyber governance processes and formerly ties cyber to the traditional NATO core task of collective defense. However, it also clarifies that NATO cyber defense exists primarily to defend its own networks and thus individual member countries are expected to defend their own national networks. It also promulgates the view that international law applies to cyberspace.[21] The governance maintains the NAC is the body that provides strategic-level oversight and "exercises principal authority in cyber defence-related crisis management."[22] Other key elements of NATO cyber governance include:

> The Cyber Defence Committee (formerly the Defence Policy and PlanningCommittee/Cyber Defence), subordinate to the NAC, is the lead committee for political governance and cyber defence policy in general, providing oversight and advice to Allied countries on NATO's cyber defence efforts at the expert level. At

> the working level, the NATO Cyber Defence Management Board (CDMB) is responsible for coordinating cyber defence throughout NATO civilian and military bodies. The CDMB comprises the leaders of the policy, military, operational and technical bodies in NATO with responsibilities for cyber defence.[23]

However, how would this governance process be applied to determine the appropriate response to any perceived aggression in cyberspace against NATO or one of the Alliance members? According to Jason Healey and Klara Tothova Jordan of the Atlantic Council's Cyber Statecraft Initiative, "This process for engagement begins at the technical level. If an incident has political implications, NATO's cyber defense efforts get elevated from the NCIRC to the CDMB and CDC [Cyber Defence Committee] through to the NAC."[24] The NAC would determine the appropriate level of response, which could include invoking collective defense through Article 5 of the NATO Charter, although this is considered unlikely unless there is significant physical damage or deaths involved.[25] Within the constructs of international law, the NATO charter, and the United Nations charter there remains general ambiguity as to exactly how an incident in cyberspace may be considered an act of war.[26] If indeed the decision is made to pursue military action in the cyberspace realm, what capabilities are available within NATO forces to accomplish this?

NATO CYBERSPACE CAPABILITY: MILITARY FOCUS

In a June 2013 blog article, General Philip Breedlove, Supreme Allied Commander Europe (SACEUR), promulgated the need for NATO forces to fully

embrace and integrate cyber defense into their operations. Noting that NATO had endured over 2,500 cyber attacks in its networks during 2012, he declared the threat to be significant enough to drive upgrades in incident response capability.

> The idea is simple and as old as the alliance. Whether the threat comes from the barrel of a gun or from a high speed internet connection, you're not alone when your security is threatened. The destructive consequences of a cyber attack can be just as devastating as the aftermath of a conventional attack and so we as a military alliance must be prepared with appropriate response options.[27]

Consistent with its current Cyber Defence Policy, NATO's top priority is to protect its own communications and information systems (CIS) that support alliance military operations.[28] NATO also has several major supporting mission areas that include shared situational awareness in cyberspace, critical infrastructure protection (CIP), critical information infrastructure protection (CIIP), counter-terrorism, support to member countries cyber-capability development, and response to crises related to cyberspace. To explore these mission areas, let us examine the operations and planning, doctrine and methods, and training and exercises related to NATO military cyberspace activities.

Operations and Planning.

As the NAC provides policy and strategic guidance, and NATO Headquarters committees provide governance, Allied Command Operations (ACO) provides the planning and execution of all alliance operations. ACO operates at strategic, operational, and tac-

tical levels to achieve its primary mission of ensuring integrity of Alliance territory as well as supporting missions that may require deployment outside this area. Strategic level operations are directed within the Supreme Headquarters Allied Powers Europe (SHAPE) located in Mons, Belgium. Operational level operations rely on standing Joint Force Commands in Brunssum, the Netherlands (JFCBS) and in Naples, Italy (JFCNP) which operate in a similar manner as U.S. joint forces in that they may conduct operations from their permanent location or from a headquarters deployed to the theater of operations. Tactical level operations are directed by three domain-based commands: Headquarters Allied Land Command (HQ LANDCOM) in Izmir, Turkey, Headquarters Allied Maritime Command (HQ MARCOM) in Northwood, U.K., and Headquarters Allied Air Command (HQ AIRCOM) in Ramstein, Germany. Support of operational command and control comes from the CIS Group headquartered in Mons, Belgium, with signal battalions in Germany, Italy, and Poland.[29] The force structure is organized in three broad categories, which are in decreasing order of readiness level: in-place forces, deployable forces, and long term build up forces.[30]

The organization of NATO cyber operations follows a similar paradigm. Strategic-level cyber defense and situational awareness occurs at ACO and operational-level cyber activities occur at the JFCs, tactical commands, and CIS Group.[31] Tactical-level cyber situational awareness is primarily provided by the NATO Communications and Information Agency (NCI Agency), an agency established in July 2012 as a merger of more than five separate NATO entities to help achieve unity of effort.[32] NCI Agency supports routine daily ACO operations and during crisis response ACO prioritizes the NCI Agency efforts. While

the NCI Agency primary mission is to connect and defend Alliance networks, it also assists NATO and Partner Nations develop interoperable communication and information capabilities.[33]

To provide NATO with constant and integrated cyber defense coverage, the NCI Agency operates technical elements of the NCIRC.[34] Initially envisioned in the 2002 Prague Summit to be "the Alliance's 'first responders' to prevent, detect, and respond to cyber incidents,"[35] the NCIRC developed its initial capabilities between 2003 and 2006 and then continued to evolve in both its capacity and capability.[36] The term "full operational capability (FOC)" has been applied to the NCIRC in several contexts. For example, the 2010 Lisbon and 2012 Chicago summits pushed for FOC by the end of 2012. As noted by one of the key project managers, "'full operational capability' is perhaps a misnomer—cyberthreats are constantly evolving, and we [NATO] will never have a final or full capability."[37] Capabilities have improved steadily as the NCIRC FOC was implemented in planned increments.[38] The FOC achieved in May 2014 at a cost of €58 million (U.S. $74.5 million) now provides improved cyber protection of 55 NATO sites worldwide.[39]

Part of the NCIRC FOC Project was the establishment of a rapid reaction team (RRT) capability by the end of 2012. The RRT capability consists of a permanent core of six cyber experts as well as national or NATO experts in other areas unique to the specific mission that can be formed to respond within 24 hours of an incident.[40] The RRT participates in NATO-sponsored exercises to hone the skills of its members and to refine its procedures. The limited nature of the RRT resources requires the team to work with industry as well as with the Computer Emergency Response Teams (CERTs) of affected nations.[41]

The NCIRC also has a staff-run Coordination Center, which coordinates cyber defense activities within NATO as well as provides staff support to the CDMB and liaison to external organizations, such as the European Union (EU).[42] One area of such collaboration is that of CIP, a challenge that is not limited to military operations alone. As one cyber subject matter expert at the NATO Joint Warfare Centre argues:

> Some military professionals argue that protecting cyberspace where civilian infrastructure operates is a civil matter, however, if an attack against infrastructure can affect the military operation, it has to be regarded in the Operational Planning Process.[43]

Certainly, NATO has made great strides in the area of its own CIIP[44] through such accomplishments as the NCIRC FOC, but how can and should NATO cyber operations support the more general threat of CIP?

In December 2012, the NATO Emerging Security Challenges Division in Brussels sponsored a conference focused on NATO's role in CIP. Findings of the meeting included the recognition that NATO's role might necessitate many response capabilities for CIP that involve such activities as disaster relief and anti-terrorism perhaps coordinated with cyber defense. However, the conference sponsor noted:

> NATO cannot be the sole answer or panacea to many of the challenges of critical infrastructure but the Alliance cannot afford to turn its back on them entirely if it seeks to remain a relevant security organization in the 21st century.[45]

One of the key concerns noted by attendees was how to define and prioritize the CIP assets among allies, as well as how to include private business.[46] These issues can be addressed, in part, through the proper planning of military operations.

Traditional military planning requires inputs and coordination amongst staff elements at the appropriate headquarters. For current cyberspace activities at Headquarters NATO, coordination may involve staffs of the J2 (Intelligence), J3 (Operations), J5 (Plans and Policy), J6 (Consultation, Control and Communications), and J7 (Cooperation and Regional Security Division) and activities at lower-level headquarters will likely involve similar staff structures. One of the greatest challenges for NATO is akin to that faced by U.S. forces with regard to which staff element leads the effort—that is, who's in charge? Although no standard NATO organization structure for cyber defense planning has been codified, common themes have emerged from exercises. One recommendation is to follow the traditional goal "to establish cross-functional staff entities to harness expertise for application and focus to cyber problems."[47] It is also prudent to develop concepts that mirror some traditional joint task force staffs, such as a Cyber Defence Cell and Cyber Defence Working Group as vehicles to facilitate coordination.[48]

When actually engaged in operations, a Joint Task Force commander must try to maintain the necessary operations tempo despite cyber attacks aimed at disrupting this objective. Thus, operational planning should fully understand and appreciate the vulnerabilities as well as the enhancements that cyberspace capabilities may present. As noted in the Joint Warfare Centre *Three Swords Magazine*, "operationally-minded decisions must prevail in determining how best to

avoid, mitigate and prevent the consequences of cyber attacks on these vulnerabilities [that are caused by operation's cyber dependencies]."[49]

In addition to operational planning, NATO must incorporate cyberspace requirements into its resource planning process. In April 2012, cyber defense was integrated into the NATO Defence Planning Process (NDPP).[50] To get the most from resource expenditures, NATO has introduced an initiative—Smart Defence—to leverage the sharing of capabilities in a time of austerity. Put simply, "Smart Defence is a cooperative way of generating modern defence capabilities that the Alliance needs, in a more cost-efficient, effective and coherent manner."[51] The initiative includes projects for enhanced cyber defense. In April 2015, the Portuguese Ministry of Defence hosted the first Cyber Defence Smart Defence Projects' Conference, which included presentations on the three projects in work, as well as sessions on cooperation with academia and industry. The first project is the Malware Information Sharing Platform (MISP), an initiative led by Belgium to "facilitate information sharing of the technical characteristics of malware within a trusted community without having to share details of an attack."[52] The MISP capability was initially designed to support NCIRC Technical Centre work but is now available to all member countries.[53]

The second project, Multinational Cyber Defence Capability Development (MN CD2), is an effort started in March 2013 and led by the Netherlands teamed with Canada, Denmark, Norway, and Romania. The project goal is to "cooperate on the development of: improved means of sharing technical information; shared awareness of threats and attacks; and advanced cyber defence sensors"[54] MN CD2 activities are managed in several work packages; the four initial work

packages are Technical Information Sharing,[55] Cyber Defence Situational Awareness (CDSA),[56] Distributed Multi-sensor Collection and Correlation Infrastructure (DMCCI),[57] Cyber Information and Incident Coordination System (CIICS) Enhancements.[58] Two new MN CD2 work packages were approved in June 2015: CIICS Support Work Package and a Cyber Security Assessment Team (CSAT) capability.[59]

The third project, Multinational Cyber Defence Education and Training (MN CD E&T), helps to develop courses for cyber education programs, battle lab support for training, and cyber range support for exercises to enhance professional development and certification of cyber defense personnel. Led by Portugal, there are 11 NATO countries formally participating with another 11 countries, as well as the EU, who are interested; currently, the United States is not among the group.[60]

Capabilities and lessons learned from these Smart Defence programs are being applied to support the broader Connected Forces Initiative (CFI) to enhance interconnectivity and interoperability of Allied forces. Together, these programs support the NATO Forces 2020 goal: "a coherent set of deployable, interoperable and sustainable forces equipped, trained, exercised and commanded to operate together and with partners in any environment."[61] Details of the CFI were outlined in the 2014 NATO Wales Summit Declaration and they include the large-scale (25,000 personnel) exercise Trident Juncture.[62] For this exercise, cyber defense experts from the NATO Joint Warfare Centre plan to practice skills and techniques that were refined through the STEADFAST series of NATO exercises.[63] What doctrine and methods form the basis for how operators will perform in these exercises?

Doctrine and Methods.

Allied Command Transformation (ATC) is one of two strategic commands of NATO; together with ACO they form the NATO Command Structure (NCS). While ACO focuses on current operations, ACT concentrates on transformation initiatives for NATO military structure, forces, capabilities, and doctrine. Headquartered in Norfolk, Virginia, ACT directs three major units: the Joint Warfare Centre in Stravanger, Norway; the Joint Force Training Centre in Bydgoszcz, Poland; and the Joint Analysis and Lessons Learned Centre in Monsanto, Portugal. Other NATO education and training centers and Centres of Excellence (COE) coordinate their activities with ACT. [64]

The only NATO accredited COE dedicated to cyberspace activities is the Cooperative Cyber Defence Centre of Excellence (CCD COE) located in Tallinn, Estonia. The CCD COE was established in October 2008 via a Memorandum of Understanding amongst seven NATO countries (Estonia, Germany, Italy, Lithuania, Latvia, the Slovak Republic, and Spain) with a vision "to enhance cooperative cyber defence capabilities of NATO and NATO nations, thus improving the Alliance's interoperability in the field of cooperative cyber defence."[65] Through its myriad endeavors, the CCD COE supports NATO education, training, exercise, and research programs. These efforts include an annual conference on Cyber Conflict first held in 2009; numerous cyberspace-related workshops and short courses addressing issues from tactical technical procedures up through national-level strategic planning; annual dedicated cyber exercises first held in 2010 as well as support to large-scale NATO exercises; and an extensive on-line library.[66]

Two other NATO-accredited COEs sponsor cyber-related activities related to maritime operations and defense against terrorism. The Combined Joint Operations From The Sea Centre of Excellence (CJOS COE) in Norfolk, Virginia, has an ongoing Maritime Cyber Security project to "lead the development of a networked response to maritime cyber security threats and challenges."[67] The center has produced white papers on the cyber defense aspects of maritime operations and port security as well as the related legal implications.[68] The Centre of Excellence Defence Against Terrorism (COE-DAT) in Ankara, Turkey, has developed and delivered various courses and workshops regarding terrorist activities in cyberspace.[69] The COE-DAT sponsored its first cyberspace-related course, "Countering Cyber Terrorism," in November 2006, which included participants from 18 countries (9 NATO and 9 non-NATO).[70] The center's most recent courses include "Terrorist Use of Cyberspace" in May 2014[71] and "Critical Infrastructure Protection against Terrorist Attacks" in November 2014;[72] both courses explored a diverse variety of cyberspace-related topics on the physical and virtual environments.

The state of doctrine development for cyberspace operations is still in the formative stages. A search through publicly available NATO Allied Joint Doctrine documents reveals an incomplete incorporation of cyberspace activities. The capstone document for Allied Joint doctrine, AJP-01 (December 2010), recognizes "cyber-operations" as an extension of traditional NATO security challenges; highlights the increase in reliance of Alliance operations on information systems and the resulting vulnerability to cyber attacks; and depicts cyber operations as a subset of defensive information operations.[73] Even though it was published 4 months after the current AJP-01, the capstone

document for communication and information systems doctrine, AJP-6 (April 2011), contains no explicit mention of "cyber" or "cyberspace." Instead, AJP-6 focuses on security aspects of communication and information systems in the guise of "Information Assurance" designed to "to ensure the systems and networks employed to manage the critical information used by an organization are reliable and secure, and processes are in place to detect and counter malicious activity."[74] The capstone document for operational planning, AJP-5 (June 2013), includes cyberspace as a functional area for planning on par with maritime, air, space, and land. AJP-5 also places "defensive cyber operations" amongst the means to help achieve coherence and synergy in the planning for joint targeting and the employment of joint fires.[75]

For operational doctrine, the relevant capstone document, AJP-3 (March 2011), has an inconsistent incorporation of cyberspace. The publication initially depicts cyberspace as a subset of the information environment, but later puts it on par with other joint capabilities in the statement:

> A joint operation endeavours to synchronize the employment and integration of the capabilities provided by land, maritime, air, space, cyber space, special operations and other functional forces.[76]

AJP-3 maintains the perspective of cyberspace as its own domain when describing the elements of a Joint Force Commander's establishing directive,[77] but then places it back under the information environment in the description of The Operational Environment.[78]

Currently, there is no dedicated NATO doctrine for cyberspace operations akin to the U.S. Joint Publication 3-12(R), *Cyber Operations* (October 2014); most of the

details of such activities are captured in AJP-3.10, *Allied Joint Doctrine for Information Operations*(November 2009). AJP-3.10 uses the nomenclature of computer network operations (CNO) and computer network defense (CND) that was used in U.S. joint doctrine prior to the release of JP 3-12(R).[79] In efforts to improve this situation, the NATO Joint Warfare Centre notes there is ongoing work "to develop a JTF HQ SOP [standard operating procedure] 218 for Cyber Defence, which will likely serve to identify pre-doctrinal processes and standard working methods before doctrine is in place."[80] Also, the cyberspace doctrine is evolving through lessons learned from various NATO exercises, as illustrated by the development of key planning products such as a Cyber Prioritized Asset List (CPAL), Cyber Risk Assessment Matrix (CRAM), and Warning Advice and Reporting Points (WARP).[81]

The continued development of cyberspace future doctrine should consider not only military capabilities, but also those of industry as well considering that the NCI Agency website states "80% of our [the NCI Agency] work is done through contracts with national Industries."[82] To facilitate enhanced relationships with commercial cyberspace ventures, the NATO Industry Cyber Partnership (NICP) was launched on September 17, 2014 at a 2-day conference in Mons, Belgium, with 1,500 industry leaders and NATO policy makers.[83] The key principle of the NICP initiative is that the NCI Agency "will cooperate with the private sector for the primary purpose of reinforcing the protection of NATO's own networks."[84] The NICP builds upon existing cooperative efforts, such as guidelines for information sharing at the technical level to enhance cyber security.[85] Recent NICP accomplishments include the successful conclusion of the Cyber Security Incubator Pilot Project in which:

NATO, industry, and academic participants worked together on defining challenges and investigating innovative solutions in the areas of big data and data fusion, cyber defence situational awareness, and mobile security.[86]

Another recent NICP partnership is one between the NCI Agency and Microsoft as part of the company's Government Security Program (GSP) to "evaluate and protect existing systems and maintain more secure infrastructure."[87]

The Multinational Capability Development Campaign (MCDC) effort for 2013-2014 is a recent venture involving many NATO countries designed to develop and refine fundamental processes to integrate cyberspace operations into operational doctrine. As the seventh iteration in a Multinational Experimentation series that started in 2001, the theme for MCDC 2013-2014 was Combined Operational Access.[88] Participants from 19 countries focused "on the versatile, agile capabilities required to project combined forces into an operational area with sufficient freedom of action to accomplish the mission."[89] The project is divided across seven Focus Areas, which included Cyber Implications for Combined Operational Access (CICOA). This is an effort of 14 contributing countries led by Italy and Norway to "develop procedural and technical solutions to facilitate the integration of cyber into the operational planning process."[90] Tasks were separated into two workstrands: one led by Norway to explore "Operational Planning and the Cyber Domain" and the other led by Italy to study "Cyber Capabilities and Data Analysis." Anticipated deliverables under review include guidelines and a handbook to support joint operational planning processes, to include

the ACO Comprehensive Operations Planning Directive (COPD). CICOA products also include guidelines and taxonomy for data analyses that support cyber situational awareness and threat assessment as part of the intelligence process.[91] The current program of work for MCDC 2015-2016 includes a focus area on Multinational Defensive Cyber Operations (MDCO) led by the United States to build upon previous work and "to develop a quicker way to effectively integrate multinational forces to conduct defensive cyber operations" for the Multinational Force Commander.[92] What are some practical means, short of actual crisis, where doctrine and processes such as that produced by the MCDC/CICOA undertaking can be learned, applied, and perfected?

Education, Training and Exercises.

Cyberspace-related education and training occurs at multiple levels throughout NATO. The NATO Defense College in Rome, Italy, addresses cyber defense issues at the strategic level, focusing on their broader geopolitical implications. In December 2013, the College hosted a forum on "NATO and the Future of Cyber Security" designed to promote a dialogue within NATO and the international security community.[93] The College's Research Division also publishes papers on cyberspace topics, such as lessons learned from the 2007 Estonia attack, future threats, and doctrine development.[94] The NATO School in Oberammergau, Germany, currently provides six resident courses related to cyber and information operations at the operational level to support NATO staff officers and network security personnel.[95] The NATO Joint Warfare Centre provides training for joint and operational-

level headquarters to include awareness and appreciation for the implications of cyberspace activities in NATO operations.[96] The NATO Communications and Information Systems School (NCISS), which became part of the NCI Agency in July 2012, provides five cyber-related resident courses for CIS operators and staff personnel. It also provides support to deployed operations and subject matter expertise for exercises, conferences, and workshops.[97] The skills achieved by personnel through education and training can be tested at the Cyber Range operated by Estonian Defence Forces and adopted for NATO use in June 2014.[98] The Cyber Range capability provides an excellent foundation for NATO cyberspace-related exercises.

NATO approaches cyberspace-related exercises in two broad categories—those specific to cyber operations and those integrated into existing exercises.[99] The largest NATO cyber defense exercise is the "Cyber Coalition" series that has been conducted annually since 2008. Cyber Coalition 2014 involved "over 600 technical, government, and cyber experts operating from dozens of locations from across the Alliance and partner nations" as well as observers from academia and industry. The exercise also served as a testbed for the CIICS product from the Smart Defence initiative.[100] Cyber Coalition 2014 also "provided a stage for exercising strategic- and operational-level information sharing, senior-level decision making, and multidisciplined coordination in the cyber realm" amongst 26 Allied and five partner nations participating.[101] The exercise control staff was hosted by the Estonian National Defence College in Tartu, Estonia and utilized the newly adopted NATO Cyber Range there.[102] Tartu also hosted Cyber Coalition 2013.[103] It is interesting to note that Cyber Coalition 2012 was run concur-

rently with the annual NATO Crisis Management Exercise (CMX), an internal command post exercise that does not involve deployed forces.[104]

In addition to the Cyber Coalition exercises, the CCD COE in Tallinn, Estonia, has sponsored the dedicated annual cyber exercise, Locked Shields, since 2010 (initially called Baltic Cyber Shield). Having grown significantly over the years, Locked Shields 2015 involved 400 participants from 16 nations, and was sponsored by a grant from the government of Canada.[105] The scenario included cyber attacks on the fictitious country of Berlya, possibly by the rival nation of Crimsonia. It was, perhaps, a shrewd homage to the 2007 cyber attacks on Estonia typically attributed to Russia, but never proven conclusively.[106] From its outset, the Locked Shields exercises have involved scenarios that include attacks on critical infrastructure. The CCD COE keeps after action reports from the exercises in its publicly accessible website library.[107]

Bolstered in part by the new strategic direction for NATO following the 2010 Lisbon Summit, the NATO Joint Warfare Centre integrated cyber defense activities into their Steadfast Juncture 2011 exercise as part of the initial effort to develop "across NATO's battlestaffs a comprehensive understanding of the far reaching impacts of cyber attack."[108] To mirror the complexity of real world cyberspace vulnerabilities, the exercise designers injected cyber attacks into three target categories: NATO command and control (e.g., computer networks); NATO operations (e.g., airports, seaports, petroleum, electricity); and NATO mission stability (e.g., energy, medical, financial, transportation, communication).[109] Two years later, life imitated the scenario as Steadfast Jazz 2013 participants experienced real-world cyber attacks during exercise activities.[110]

Cyber defense activities were also integrated into the 2014 Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX) held at the Joint Forces Training Centre in Bydgoszcz, Poland "to solve existing interoperability issues and explore and share potential solutions in anticipation of future operations and budget constraints."[111] The cumulative lessons learned from cyber experience in NATO exercises were used to inform the recent Trident Juncture 2015 exercise (TRJE15), the largest NATO exercise since 2002. The exercise was planned to be conducted from October 3 to November 6, 2015 in Italy, Portugal, and Spain.[112] As discussed earlier, TRJE15 tested many of the concepts in the NATO Smart Defence and Connected Forces Initiative to certify Joint Force Command Brunssum for command of the NATO Response Force.[113] Cyber experts from the NATO Joint Warfare Centre published a series of seven recommendations specifically aimed at applying cyber defense transformation measures gleaned from the last four STEADFAST exercises to TRJE15.[114] These exercises test operational concepts and processes that may be applied in contemporary situations within the Alliance. What are the key issues related to the current NATO cyber policy that require the thoughtful consideration of senior leaders?

KEY ISSUES FOR CURRENT POLICY

The 2010 NATO Strategic Concept represents a renaissance of NATO core tasks. The new Enhanced Cyber Defence Policy affirms the role that NATO cyber defense contributes to the mission of collective defense and embraces the notion that a cyber attack may lead to the invocation of Article 5 actions for the

Alliance. Against this backdrop, this section examines the related issues of offensive cyberspace, deterrence in and through cyberspace, legal considerations, and cooperation with the EU.

Offensive Cyberspace.

A significant "elephant in the room" issue for NATO cyberspace operations is the possibility of any use of offensive cyber by the Alliance. Cyber expert James Lewis poses this challenge as: "The central question for NATO's cyber doctrine is how the lack of an articulated offensive cyber capability affects its ability to deter or defend."[115] In general, offensive cyberspace operations may be considered as the use of cyber capabilities outside of the defensive firewall of the NATO network. Such operations could be conducted in support of tactical activities by forces in the physical domains (e.g., land, sea, or air) or the operations may be used as long-range strategic weapons directed at the military and infrastructure of another nation. The implications of the purposeful use of devastating cyber methods against a foreign homeland bring up allusions to the use of nuclear weapons. In fact, Lewis asserts that there is a "cyber club" with NATO—the United States, the United Kingdom, and France—that possess not only nuclear weapons, but also an active offensive cyberspace capability.[116] Indeed, the United States has officially incorporated offensive cyberspace operations (OCO) in its publicly available joint doctrine in general terms, but details of any OCO implementation remain classified.[117]

In practical terms, NATO may already be entering the gray zone of developing active cyber defense capabilities that go beyond the firewall to neutralize

specific Internet nodes that are conducting attacks, such as those that facilitated distributed denial of service actions experienced by Estonia in 2007. As one NATO cyber officer noted, "NATO has established a capable defence for most cyber threats, but that is just the first step and what needs to quickly follow is the development of 'active defence' capabilities."[118] In implementing such measures, decision-makers must recognize that whether acts of active cyber defense are considered offensive is not up to the sender, rather the receiver, because well-justified defensive acts may be misinterpreted as aggression.[119] However, if NATO operations do evolve to embrace active cyber defense, and then go further to adopt OCO in a manner similar to that of nuclear weapons, the issue of political control of OCO release and use must be resolved first.[120] Healey and Jordan assert that the focus should remain on offensive coordination, not capability, and suggest that NATO should create a group "with voluntary opt-in for states, modeled after NATO's existing Nuclear Planning Group, to discuss and map out an offensive cyber policy."[121]

Deterrence In and Through Cyberspace.

Closely related to the concept of OCO is what part such a capability might play in the overall notion of deterrence. Certainly, the NATO goal of achieving deterrence with the Warsaw Pact through various configurations of nuclear force planning has dominated much of both alliances' early histories. In an award-winning essay published in Joint Force Quarterly, Clorinda Trujillo surveyed existing scholarly publications and compiled a proposed list of seven cyberspace deterrent options, most of which do not require OCO. Trujillo also noted the particular bar-

riers associated with any practice application of cyber deterrence, such as the challenge of attribution as well as the risk of unintentional outcomes where the use of a cyber capability may itself result in further vulnerability.[122]

Deterrence theory usually includes the possibility of an escalation of conflict and force between parties. Traditional nuclear deterrence frameworks such as the Kahn escalation ladder have been applied conceptually to circumstances that address not only cyber, but also conventional and nuclear forces in the possible scenarios.[123] Potential misunderstanding of intentions and actions coupled with imperfect situational awareness and lack of common language may facilitate escalation. In a NATO Defense College research paper, Christine Hegenbart argues for the development of precise and actionable linguistics to facilitate understanding of a cyber conflict escalation ladder that may span a spectrum from hacktivism/cyber vandalism all the way up to cyber war.[124]

Deterrence at an international level is most effective when it utilizes all instruments of power available to a country—diplomatic, information, military, and economic. The United States may be the only country with a publicly available declaratory deterrence statement as part of its International Strategy for Cyberspace, as stated below:

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, mili-

> tary, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.[125]

Since the U.S. statement explicitly includes the protection of allies, this implies inclusion of NATO under the U.S. cyber deterrence umbrella. Even with this theoretical protection, policy makers need to consider how to deal with nonstate actors that are heavily vested in the virtual realm (e.g., Anonymous and LulzSec). Such groups may be impossible to deter since they have "a different risk tolerance than those acting in a physical domain due to their perceived anonymity, invulnerability, and global flexibility."[126]

Legal Considerations.

A continuing issue writ large within both NATO and the global community involves how existing international law applies to activities in cyberspace. From a security perspective, significant progress was made with the publication of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* in 2013, the culmination of a 3-year collaborative effort sponsored by the CCD COE.[127] The *Tallinn Manual* was preceded by the publication of *International Cyber Incidents: Legal Considerations,* an earlier study by the CCD COE that includes case studies on four high-visibility cyber attacks: Estonia 2007; Radio Free Europe/Radio Liberty 2008; Lithuania 2008; and Georgia 2008.[128]

The analytical framework within the *Tallinn Manual* is based largely on the work of Michael Schmitt, but it represents only one such model for evaluating the severity level of cyber conflict.[129] Perhaps not surprisingly, some non-NATO nations—Russia and China in particular—do not fully agree with the principles espoused within the *Tallinn Manual.* This is a significant challenge considering these countries are two of the five permanent members of the United Nations Security Council.[130]

Recognizing that the *Tallinn Manual* focuses on cyber warfare amongst state actors at levels that comprise "armed attacks," a CCD COE team is now working on how international law applies to less severe malevolent activity in cyberspace. The effort known as "Tallinn 2.0" looks at aggression below this threshold, and publication of an updated *Tallinn Manual* is anticipated in 2016.[131] In addition, the CCD COE continues to sponsor courses and workshops that facilitate better understanding of legal issues related to cyber conflict.[132]

NATO initiatives with the private sector, such as NICP, present significant legal issues regarding the status of the private contractors' civilian employees who support NATO operations. The implications regarding their vulnerability to legitimate attack as well as liability for due diligence remains under legal evaluation.[133]

Cooperation with the European Union.

The 2010 Lisbon Summit Declaration included a call for NATO to work more closely with the EU in the area of cyber defense.[134] Indeed, of the 28 NATO countries, all but Albania, Canada, Iceland, Norway,

Turkey, and the United States are members of the EU. These countries share common interests in security programs conducted by both organizations as well as the desire not to have unnecessary duplication of resource contributions. Regarding cyber security, both groups have similar goals, but different approaches, as summed up by Piret Pernik of the International Centre for Defence Studies in Estonia:

> For both NATO and the EU, cyber security is a strategic issue that impacts the security and defence of member states and of the organisations themselves. They both prioritize the resilience and defence of their own networks, organisations and missions, leaving cyber security of individual members states a national responsibility. The missions of the two organisations are complementary, with NATO focusing on security and defence aspects of cyber security, and the EU dealing with a broader, mainly non-military range of cyber issues (Internet freedom and governance, online rights and data protection), and internal security aspects.[135]

Previous NATO-sponsored studies have recommended improved cooperation between NATO and the EU in such areas as critical infrastructure protection.[136] However, unlike NATO, the EU does not provide direct technical support. Rather, it facilitates information sharing through such organizations as the European Network and Information Security Agency (ENISA) and the European Defence Agency (EDA).[137] Other significant differences between the two groups is that the EU does not own its command and control information systems and it lacks the central authority for common cyber security, such as that found in the NAC.[138]

In November 2014, the Council of the EU adopted the EU Cyber Defence Policy Framework to identify priorities as well as roles and responsibilities related to the EU Common Security and Defence Policy.[139] Section five of the framework, "Enhancing cooperation with relevant international partners," includes a description of methods to improve EU and NATO collaboration in cyberspace:

> There is a political will in the EU to cooperate further with NATO on cyber defence in developing robust and resilient cyber defence capabilities as required within this Policy Framework. Regular staff-to-staff consultations, cross-briefings, as well as possible meetings between the Politico-Military Group and relevant NATO committees, shall help to avoid unnecessary duplication and ensure coherence and complementarity of efforts, in line with the existing framework of cooperation with NATO.[140]

SUMMARY OF FINDINGS

This section summarizes the key findings from the discussion of NATO cyberspace capabilities and briefly examines how they apply to U.S. Department of Defense (DoD) and U.S. Army cyberspace activities in Europe.

1. The NATO institutional embrace of cyberspace activities is similar to other forms of evolution that the Alliance has undergone since its formation.

Aspects of the evolution of U.S. military cyberspace goals parallel similar developments in NATO. U.S. Cyber Command reached its full operational capability and U.S. Army Cyber Command was established during the month before the Lisbon Summit's call

for an in-depth update of NATO cyber policy.[141] This policy was approved by NATO Defence Ministers in June 2011, just a month before the release of the *DoD Strategy for Operating in Cyberspace*.[142] Most recently, the endorsement of an enhanced NATO cyber policy at the September 2014 Wales Summit was followed by an updated DoD cyber strategy in April 2015.[143]

U.S. European Command (USEUCOM) has also evolved to adopt cyber operations into its J6 staff element, officially named the Command, Control, Communications and Computer (C4)/Cyber directorate. Among its current priorities is "Operationalizing the Joint Cyber Center capabilities (synchronization and integration)." In his February 2015 testimony to Congress, the USEUCOM Commander, General Philip Breedlove, noted two significant milestones for his theater's cyberspace capabilities:

> EUCOM's first Cyber Combat Mission Team (CMT) and Cyber Protection Team (CPT) reached Initial Operational Capability (IOC) this past year providing us with new capabilities to protect our people, systems, information, and infrastructure while holding adversaries at risk. As these teams continue to improve, EUCOM will have an enhanced ability to plan and conduct Cyberspace Operations to enhance our situational awareness and protect our cyber flank.[144]

U.S. Army Europe (USAREUR) continues to support the changing requirements for not only USEUCOM, but U.S. Africa Command as well. In July 2014, the 5th Signal Command opened the Gray Center Cyber Operations Center in Wiesbaden, Germany. The center is designed "to consolidate tactical, theater and strategic communications" for combatant commanders and Army forces and it has a long-term

goal "to take over cyberwatch responsibility from the Stuttgart-based European Command."[145] Toward this goal, the center includes a Theater Cyber Operations Integration Center.

2. Despite a call at the 2010 Lisbon Summit to incorporate the cyber dimension into NATO doctrine, the process has been slow and inconsistent. The relationship between cyberspace and information operations in doctrine is unclear. The focus of NATO cyberspace in doctrine (formal and de facto) is defensive and supportive in nature; this appears to be by design since NATO has yet to adopt or coordinate any position on the use of any offensive cyber activity.

General Breedlove's February 2015 testimony to Congress discussed cyberspace operations and information operations as distinct capabilities that complement each other.[146] The United States should encourage NATO doctrinal development to follow the current DoD model that distinguishes cyberspace operations from information operations in separate joint publications (JP 3-12 and JP 3-13, respectively).

At the Service level, the Army is working to implement the joint doctrine structure through updates in field manuals and related training. In September 2015, the Army Cyber COE formalized this as an initiative in its Strategic Plan: "Establish Foundational Doctrine for Army Cyberspace Operations That Is Consistent With Joint Doctrinal Tenets." This initiative includes the development of Field Manual (FM) 3-12, "Cyberspace Operations," that will supersede FM 3-38, "Cyber Electromagnetic Activities."[147] During this transition period, the Army should continue to work with NATO nations to share expertise on the evolving role

of cyberspace activities. A good example of such cooperation is represented by the certificate of partnership signed in March 2015 by Major General Stephen, Commanding General of the Army Cyber COE, and Major General Heinrich-Wilhelm Steiner, Commander of the German Bundeswehr Communication and Information Systems Command.[148]

3. The role of cyberspace activities in NATO deterrence operations is not yet defined in any public forum.

As noted, NATO cyberspace forces do not have offensive capabilities by design. Thus, some theorists may argue that cyberspace operations cannot contribute to NATO deterrence. A recent Defense Science Board Task Force conducted a detailed study "to review and make recommendations to improve the resilience of DoD systems to cyber attacks," and the group's final report offers several insights that should be considered by NATO political and military leaders.[149] The Task Force report's first recommendation is to "Protect the Nuclear Strike as a Deterrent (for existing nuclear armed states and existential cyber attack)," which would be applicable to a limited number of state actors that may pose a credible and attributable high-tier threat.[150] If adopted by NATO, the schema could leverage the existing NATO nuclear force structure to provide deterrence against existential-level cyber attacks.

Perhaps a more tempered and balanced approach is offered by the same report's second recommendation: "Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary."[151] In contrast to the focus of the first rec-

ommendation on the extreme end of the attack spectrum, the report asserts, "this strategy [of the second recommendation] builds a real ladder of capabilities and alleviates the need to protect all of our systems to the highest level requirements."[152] As U.S. political and military leadership wrestles with the methods best suited to achieving deterrence using all forms of national power—including cyberspace capabilities—they should continue to factor in the deterrence provided indirectly to NATO.

4. Cyberspace presents the Alliance with complex and interconnected challenges such as critical infrastructure protection at the NATO and national level. Many nations face further challenges in coordinating and integrating their own internal whole-of-government approaches.

Certainly, the United States is among those nations striving to develop and maintain a national cyberspace defense that is coordinated across federal, state, and local government. While self-interest is a necessity for any sovereign country, there are areas of cyberspace activity where prudent measures and harmonized actions work to the benefit of international security and stability. Toward this end, the April 2015 *Department of Defense Cyber Strategy* identifies Europe as a priority region for partnership building and explicitly calls for DoD to "work with key NATO allies to mitigate cyber risks to DoD and U.S. national interests."[153]

At the combatant command level, USEUCOM has sponsored the annual Exercise Combined Endeavor for 20 years as part of the U.S. investment in improved regional C4 interoperability. The exercise is evolving to integrate cyber defense into a shared mission network infrastructure that can accommodate a "bring

your own device" environment.[154] However, such exercises can only test capabilities developed and honed well in advance. Cooperation among partner nations is enhanced through opportunities such as the July 2015 Cyber Summit sponsored by USAREUR, which had a theme that discussed "how to protect critical networks and infrastructure, but still achieve interoperability with allies in the cyber domain."[155]

5. NATO has established robust education, training, and exercise programs that include dedicated cyber exercises as well as ones integrated into large-scale exercises addressing both the political and military aspects of crisis management.

A thorough education, training, and exercise program for cyberspace should address people and programs at all levels within NATO. At the garrison level, USAREUR has an excellent awareness and training program, available on their public website, that addresses information assurance aspects of cyber security as well as operational security and force protection.[156] The repository includes a superb presentation on "The Cyber Attack Cycle" that discusses the seven-step process of most cyber attacks developed by the Army Provost Marshal General in collaboration with the Army Cyber Command.[157]

With a solid foundation at the unit level, USAREUR forces also work to establish tactical-level interoperability through events such as the annual "Stoney Run" exercise between the Bravo Company, 44th Expeditionary Signal Battalion and the 250 Gurkha Signal Battalion. Lessons learned from NATO support of the Afghan Mission Network have been applied to develop the Army Coalition Mission Environment, which

will be integrated into the Steadfast Cobalt 15 exercise in Poland. Cooperative efforts between the USAREUR 102nd Signal Battalion and the 282nd Bundeswehr Command Support Battalion strive to work out cultural challenges amongst partner nations resulting from differences in language, planning cycles, and societal values.[158]

At the NATO operational level, USEUCOM conducts exercises such as Combined Endeavor 2014, which involved 30 nations and three international organizations that spent "three weeks training, operating, and configuring to a common securable standard."[159] In addition to large-scale exercises, USEUCOM also supports the education of key leaders within NATO. In December 2014, the George C. Marshall Center in Garmish-Partenkirchen, Germany conducted its inaugural Program on Cyber Security Studies with 67 participants from 47 countries. These attendees all had "professional knowledge and capabilities to deal with transnational cyber security challenges" and the course material was "tailored for senior officials responsible for developing or influencing cyber legislation, policies or practices in their countries." As part of the agenda, the USEUCOM/J6, Brigadier General Welton Chase Jr. "discussed mutual training opportunities and exercises to enhance cyber capabilities, interoperability and resiliency."[160]

6. NATO has done well to include industry, partner countries, and organizations such as the EU in many of their cyber-related activities.

To help promulgate partnerships beyond military-to-military venues, USEUCOM developed Cyber Endeavor as its "paramount cyber security collabora-

tion, familiarization, and engagement program" that includes participation by academia and industry.[161] Cyber Endeavor began in 2009, and it is comprised of a series of regional seminars held in different countries with speakers from the military, academia, and companies such as Microsoft, Hewlett Packard, Cisco, and Verizon. Cyber Endeavor 2014 held seminars in three NATO countries: the Czech Republic, focused on configuration management; Bulgaria, focused on vulnerability management; and Romania, focused on boundary defense. The 2014 program culminated with a capstone seminar in Grafenwöhr, Germany, held concurrently with exercise Combined Endeavor, but separate from its activities. The capstone agenda was split equally into two major elements, with one half comprised of presentation and discussions on the latest trends in cyberspace activities and the other half concentrated on hands-on training.[162]

7. NATO cyber activities have provided smaller countries with unique leadership roles within the Alliance.

In general, U.S. engagement with smaller NATO countries on cyberspace issues has been positive and encouraging. As noted earlier, Cyber Endeavor seminars have been conducted in smaller NATO countries as well as Partnership for Peace countries, such as Montenegro.[163] The USEUCOM International Cyber Engagement team recognized the opportunity to leverage existing programs, such as the State Partnership Program, to involve National Guard units in the development of cyber capabilities of specific nations. One example is the coordination with the Albania J6 staff and the New Jersey National Guard in May 2012 that followed a successful Cyber Endeavor seminar in Tirana in March of that year.[164]

There have been occasions when the United States has been slower to participate in new NATO cyberspace undertakings led by smaller countries. For example, the United States did not join the CCD COE until November 2011, more than 3 years after its founding in Estonia.[165] In addition, there was no active U.S. participation in the MCDC 2013-2014 CICOA cyberspace initiative, although as noted earlier, the United States has taken a lead role in the MCDC 2015-2016 MDCO initiative.[166] While it may not always be possible or prudent to have U.S. leadership in every area of NATO cyberspace programs, it is advisable for USEUCOM and USAREUR leadership to evaluate and prioritize future NATO engagement opportunities promptly.

8. NATO has taken a lead role on a global scale in establishing standards for legal evaluation of activities in cyberspace.

The United States had an active role in the development and review of the original *Tallinn Manual*, with Professor Michael Schmitt of the Naval War College serving as Director of The International Group of Experts. The U.S. participation included an observer from U.S. Cyber Command and reviewers from the Naval Postgraduate School and the U.S. Military Academy.[167] Representatives of the Naval War College also provide lectures as part of the law courses offered by the CCD COE.

The review of contemporary legal issues related to cyberspace continues to be addressed in several Service-specific journals such as the U.S. Naval War College *International Law Studies*[168] and *The Air Force Law Review*.[169] Also, The Army Cyber Institute at West

Point and U.S. Marine Force Cyberspace Command jointly produce *The Cyber Defense Review* to serve "as the leading online and print journal for issues related to cyber for military, industry, professional and academic scholars, practitioners and operators" that addresses topics of law, ethics, and policy as well as strategy, operations, tactics, and history.[170]

9. Cyberspace efforts must compete for resources with other operations and initiatives within NATO.

Simply put, cyberspace activities are not the number one priority for NATO, and perhaps not even in the top ten. In his May 2015 assessment of the Wales Summit, European expert Dr. John Deni argues that one of the key obstacles facing the NATO refocus on core missions is "the imbalance between an increasing number of missions and stagnating resources."[171] He further warns that in such a constrained fiscal environment, "the clear risk here is that NATO may over-commit and over-extend itself" in the pursuit of six new initiatives which do not include existing efforts in cyber security as well as those in energy and environmental security.[172]

Indeed, in his March 2013 testimony to Congress, former SACEUR and USEUCOM commander Admiral James Stavridis listed cyberspace as only one of six transnational threats, which, in turn, collectively comprised the fourth of his six theater priorities for USEUCOM.[173] The current SACEUR, General Philip Breedlove, in his 2014 article "The New NATO" listed cyber security challenges in a group of "also need to consider threats" toward the end of the discussion.[174] This is not to imply that cyberspace capabilities are not important to NATO. Rather, it is to acknowledge

the numerous competing tasks facing the Alliance as it continues to evolve in a complex and dynamic international environment.

The realm of cyberspace itself will continue to change, as will the myriad actors that operate in and through it for purposes related to all instruments of power. NATO cyberspace activities face many challenges that must be assessed and prioritized on a recurring basis by policymakers. While there will always be room for improvement, the overall state of cyberspace activities within NATO appears to be sound. The continued resourcing for, and pursuit of, improved cyberspace capabilities by U.S. military forces in Europe will help to ensure the steady progress of NATO cyberspace endeavors.

ENDNOTES

1. "Prague Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague on 21 November 2002," NATO Press Release (2002)133, North Atlantic Treaty Organization, November 21, 2002, available from *nato.int/docu/pr/2002/p02-127e.htm*, accessed September 8, 2015.

2. Sverre Myrli, Rapporteur, "NATO and Cyber Defence," 2009 Annual Session Document 173 DSCFC 09 E BIS, NATO Parliamentary Assembly, November 2009, para. 46, available from *www.nato-pa.int/default.Asp?SHORTCUT=1782,* accessed August 25, 2015.

3. "Riga Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006," NATO Press Release (2006)150, North Atlantic Treaty Organization, November 29, 2006, available from *nato.int/cps/en/natolive/official_texts_37920.htm*, accessed August 25, 2015.

4. "Bucharest Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008," NATO Press Release (2008)049, North Atlantic Treaty Organization, April 3, 2008, available from *nato.int/cps/en/natolive/official_texts_8443.htm,* accessed August 25, 2015.

5. "Strasbourg/Kehl Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg," NATO Press Release (2009)044, North Atlantic Treaty Organization, April 4, 2009, available from *nato.int/cps/en/natolive/news_52837.htm*, accessed March 25, 2016.

6. "Lisbon Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon," NATO Press Release (2010)155, North Atlantic Treaty Organization, November 20, 2010, pp. 10-11, available from *nato.int/nato_static_fl2014/assets/pdf/pdf_2010_11/2010_11_11DE1DB9B73C4F9BBFB52B2C94722EAC_PR_CP_2010_0155_ENG-Summit_LISBON.pdf,* accessed August 25, 2015.

7. "Chicago Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012," NATO Press Release (2012)062, North Atlantic Treaty Organization, May 20, 2012, available from *nato.int/cps/en/natolive/official_texts_87593.htm?mode=pressrelease,* accessed August 25, 2015.

8. "Wales Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales," Press Release (2014)120, North Atlantic Treaty Organization, September 5, 2014, available from *nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease,* accessed August 25, 2015.

9. Myrli, para. 67.

10. "Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010," Strategic Concept 2010, North Atlantic Treaty Organization, November 19, 2010.

11. "North Atlantic Treaty Organization Strategic Concepts," official website, updated November 11, 2014, available at *nato.int/cps/en/natohq/topics_56626.htm*, accessed August 28, 2015.

12. "Active Engagement, Modern Defence," pp. 2-3. The core tasks of NATO are in the document as follows:

> 4. The modern security environment contains a broad and evolving set of challenges to the security of NATO's territory and populations. In order to assure their security, the Alliance must and will continue fulfilling effectively three essential core tasks, all of which contribute to safeguarding Alliance members, and always in accordance with international law:
>
> a. Collective defence. NATO members will always assist each other against attack, in accordance with Article 5 of the Washington Treaty. That commitment remains firm and binding. NATO will deter and defend against any threat of aggression, and against emerging security challenges where

they threaten the fundamental security of individual Allies or the Alliance as a whole.

b. Crisis management. NATO has a unique and robust set of political and military capabilities to address the full spectrum of crises – before, during and after conflicts. NATO will actively employ an appropriate mix of those political and military tools to help manage developing crises that have the potential to affect Alliance security, before they escalate into conflicts; to stop ongoing conflicts where they affect Alliance security; and to help consolidate stability in post-conflict situations where that contributes to Euro-Atlantic security.

c. Cooperative security. The Alliance is affected by, and can affect, political and security developments beyond its borders. The Alliance will engage actively to enhance international security, through partnership with relevant countries and other international organisations; by contributing actively to arms control, non-proliferation and disarmament; and by keeping the door to membership in the Alliance open to all European democracies that meet NATO's standards.

13. *Ibid*., p. 4. The actual text from the document describing cyber attacks within the context of The Security Environment is:

12. Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies, and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks.

14. *Ibid*., p. 5.

15. Jason Healey and Klara Tothova Jordan, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow,* Issue Brief, Brent Scowcroft Center on International Security, Washington, DC: The Atlantic Council, September 2014, p. 2. This brief is an update on a 2011 study; see also Jason Healey and Leendert van Bochoven, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, Issue Brief, Washington, DC: The Atlantic Council, 2011.

16. “Defending the networks: The NATO Policy on Cyber Defence,” NATO Policy, North Atlantic Treaty Organization, 2011, p. 1.

17. *Ibid.*

18. “Bucharest Summit Declaration,” para. 47.

19. “Defending the networks.”

20. “Wales Summit Declaration,” para. 72.

21. “NATO Summit Updates Cyber Defence Policy,” Incyder news, NATO Cooperative Cyber Defence Centre of Excellence, October 24, 2014, available from *https://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html*, accessed September 8, 2015.

22. “North Atlantic Treaty Organization Cyber Security,” official website, updated July 9, 2015, available from *nato.int/cps/en/natohq/topics_78170.htm*, accessed August 25, 2015.

23. *Ibid.*

24. Healey and Jordan, p. 3.

25. *Ibid.*, pp. 3-4. The brief provides additional details on possible decision by the NAC:

> If the incident was especially devastating, the NAC could also choose to invoke collective defense through Article 5, a process which happened quickly after the terrorist attacks on 9/11. The 2010 Strategic Concept revealed the political backing to the applicability of the concept of collective defense to the cyber domain. The Strategic Concept stated, in essence, that a cyberattack against member states could justify them turning to NATO for assistance or invoking Article 5 of the Washington Treaty.

26. See Jeffrey L. Caton, *Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations and Response Implications*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, October 2014.

27. Philip Breedlove, "Attacks from Cyberspace. . . . NATO's newest and potentially biggest threat," From the Cockpit Blog, Allied Command Operations, Supreme Allied Commander Europe website, June 10, 2013, available from *aco.nato.int/saceur2013/blog/attacks-from-cyberspacenatos-newest-and-potentially-biggest-threat.aspx*, accessed August 28, 2015.

28. "NATO Cyber Defence," Media Backgrounder, NATO Public Diplomacy Division (PDD) – Press and Media Section, October 2013, available from *nato.int/nato_static/assets/pdf/pdf_2013_10/20131022_131022-MediaBackgrounder_Cyber_Defence_en.pdf,* accessed August 21, 2015.

29. "North Atlantic Treaty Organization Allied Command Operations (ACO)," official website, updated November 11, 2014, available from *nato.int/cps/en/natohq/topics_52091.htm*, accessed September 16, 2015. Key missions for ACO are summarized as:

> ACO must ensure the ability to operate at three overlapping levels: strategic, operational and tactical, with the overarching aim of maintaining the integrity of Alliance territory, safeguarding freedom of the seas and economic lifelines, and to preserve or restore the security of NATO member countries. Moreover, in the current security environment, deploying forces further afield has become the norm.

30. "High Readiness Forces and Headquarters in the NATO force structure," Allied Command Operations official website, available from *aco.nato.int/page134134653.aspx*, accessed on September 19, 2015.

31. Rizwan Ali, "On Cyber Defence," *The Three Swords: The Magazine of the Joint Warfare Centre*, No. 26, May 2014, pp. 32-34.

32. "NATO Communications and Information Agency," NATO Communications and Information (NCI) Agency official website, available from *ncia.nato.int/About/Pages/About-the-NCI-Agency.aspx*, accessed September 19, 2015. The website summarizes the origin of the NCI Agency:

> The NATO Communications and Information (NCI) Agency was established on 1 July 2012 as a result of the merger

> of the NATO Consultation, Command and Control Agency (NC3A), the NATO ACCS [Air Command and Control System] Management Agency (NACMA), the NATO Communication and Information Systems Services Agency (NCSA), the ALTBMD [Active Layered Theatre Ballistic Missile Defence] Programme Office and elements of NATO HQ ICTM [Information Communications and Technology Management].

33. "NCI Agency Cyber Security: NATO's first line of cyber defence," official website, available from *ncirc.nato.int/*, accessed August 28, 2015. The NCI Agency mission statement is:

> To strengthen the Alliance through connecting its forces, the NCI Agency delivers secure, coherent, cost effective and interoperable communications and information systems and services in support of consultation, command & control and enabling intelligence, surveillance and reconnaissance capabilities, for NATO, where and when required. It includes IT support to the Alliances' business processes (to include provision of IT shared services) to the NATO HQ, the Command Structure and NATO Agencies.

34. *Ibid*. Specific tasks performed by the NCI Agency related to the NCIRC are:

> What we do. Combating Cyber Attacks - the Agency's Cyber Security Service Line is NATO's first line of cyber defence. It operates cyber defence capability development, the NATO Information Security Operations Centre and the NATO Computer Incident Response Capability (NCIRC) Technical Centre, providing integrated cyber defence 24/7, year round. The NCI Agency Cyber Security Service Line is also responsible for planning and executing all lifecycle management activities, including subject matter expertise, research and development, software development, acquisition and operations and maintenance.

35. Healey and Jordan, p. 1.

36. Serkan Yağu and Selçuk Dal, "Active Cyber Defense within the Concept of NATO's Protection of Critical Infrastructures," *International Journal of Social, Behavioral, Educational, Economic and Management Engineering*, Vol. 8, No. 4, 2014, pp. 11-14.

37. George I. Seffers, "NATO Set to Strengthen Cybersecurity," *SIGNAL Magazine,* Vol. 28, No. 8, August 2011.

38. *Ibid*. The NCIRC development process is summarized as:

> The effort will be implemented in several increments and will include an upgraded capability to identify, trap and analyze malware and cyberattacks launched against alliance systems; advanced sensors to provide improved early detection of threats against NATO networks; a consolidated information assurance picture that will give operators an overview of the situation across NATO networks, including a dynamic risk assessment; and an upgraded and advanced threat assessment capability.

39. Julian Hale, "NATO Steps Up Efforts To Ward Off Cyberattacks," *Defense News*, July 10, 2013, available from *defensenews.com/article/20130710/DEFREG01/307100018/*, accessed September 19, 2015.

40. "NATO Rapid Reaction Team to fight cyber attack," NATO News official website, March 13, 2012, available from *nato.int/cps/en/SID-CF294941-345E723F/natolive/news_85161.htm*, accessed September 14, 2015. The efforts necessary to establish the Rapid Reaction Team (RRT) capability are summarized as:

> So far, a number of steps have already been taken, and the NCIRC should achieve full operational capability in early 2013. All the technical requirements have been identified and a call for bids has been launched. Cooperation arrangements are being developed, involving experts among whom there is mutual confidence and who come from the nations, from industry, from academia and from NATO. These arrangements will eventually open up access to specialised expertise in all areas of cyber security. The profiles of experts needed for assistance missions, specifying the areas of competence, are also being prepared.

41. "Men in black – NATO's cybermen," NATO News official website, April 24, 2015, available from *nato.int/cps/en/natohq/news_118855.htm*, accessed September 19, 2015.

42. "North Atlantic Treaty Organization Cyber Security," official website.

43. H. Todd Waller, "Cyberspace Implications for NATO Operations and the Joint Warfare Centre," *The Three Swords: The Magazine of the Joint Warfare Centre*, No. 20, Summer/Autumn 2011, p. 23. Lieutenant Colonel Waller argues that critical infrastructure protection (CIP) presents an important supporting mission for NATO military:

> To summarize, the vulnerabilities of a NATO military operation in the cyber realm are wide and far reaching. While attacks on NATO networks are possible and the type for which military forces are most prepared, an attacker may choose something other than a hardened military network. Attacks against less secure civilian networks and infrastructure might be easier and offer more tangible results. This presents unique challenges for a traditional defence apparatus designed to achieve superiority in physical space, not cyberspace.

44. Bart Smedts, *NATO's Critical Infrastructure Protection and Cyber Defence*, Focus Paper 19, Brussels, Belgium: Center for Security and Defence Studies, The Royal High Institute for Defence, July 2010. See pp. 13-18 of this report for a concise description of the NATO framework for critical information infrastructure protection (CIIP).

45. "The World in 2020 – Can NATO Protect Us? The Challenges to Critical Infrastructure," Conference Report, NATO Emerging Security Challenges Division, December 10, 2012, p. 34. These remarks were made by Jamie Shea, Deputy Assistant Secretary General, Emerging Challenges Division, as part of the conference conclusion.

46. *Ibid*., p. 10. During the conference, Lieutenant General Walter E. Gaskin, the Deputy Chairman of the Military Committee, NATO, noted the need to clearly define scope and terms for CIP:

> The evolution of the international security environment added a new layer of less predictable threats from a group of often non-state actors that can hardly be directly engaged. In this context critical infrastructure can be disrupted or

> damaged while it is very difficult to identify and counter the perpetrators' attack. Therefore, we need to consult on a common definition of critical infrastructure in order to identify our most valuable assets and analyze individual as well as shared vulnerabilities. Finally, we need to assign clear responsibilities of protection to the various stakeholders on the national and international level as well as include the private business community.

47. Peter Hutson, "Cyber Defence in Operations," *The Three Swords: The Magazine of the Joint Warfare Centre*, No. 26, May 2014, p. 36.

48. *Ibid*., p. 37.

49. H. Todd Waller, "On the Road of Cyber Defence Transformation," *The Three Swords: The Magazine of the Joint Warfare Centre*, No. 23, August 2012/February 2013, p.20. The author also recommends a holistic approach to planning that involves cyberspace activities:

> A third step in cyber defence transformation is realizing the treatment for cyber vulnerabilities is not always a computer or network solution. Since the NRF commander's resources to support non-NATO networks will be limited during an operation, other solutions need to be considered, for example, planning operations in a way that limit dependence on vulnerable computer systems. Operational planners are perhaps the best equipped to understand the link between the operational design and its various cyber dependencies, and to know what are the feasible alternatives to limit the operation's cyber exposure. (p. 19)

50. "North Atlantic Treaty Organization Cyber Security," official website.

51. "Smart Defence," NATO official website, last updated September 1, 2015, available from *nato.int/cps/en/natohq/topics_84268.htm*, accessed on September 15, 2015.

52. "Sharing malware information to defeat cyber attacks," NATO News official website, November 29, 2013, available from *nato.int/cps/en/natohq/news_105485.htm,* accessed September 17, 2015.

53. *Malware Information Sharing Platform*, Factsheet, Brussels, Belgium: NCI Agency. The factsheet describes MISP as follows:

> MISP – Malware Information Sharing Platform is a combination of a community of members, a knowledge base on malware, and a web-based platform. It is a practical and successful instantiation of the Smart Defence concept and is fully coherent with all current NATO Cyber Defence information sharing initiatives.
>
> It combines a searchable repository with a multidirectional information sharing mechanism. Where possible, MISP also provides automation mechanisms that enable the automatic import and export of data and the interfacing with other systems. The aim is to speed up the detection of incidents and the production of defence countermeasures, especially for malware that is not blocked by anti-virus protection, or that is part of sophisticated targeted intrusion attempts.

54. "NATO Nations launch Multinational Cyber Defence (MN CD2) Project," MN CD2 – Cyber Defence Capability Development official website, March 14, 2013, available from *https://mncd2.ncia.nato.int/news/Pages/MN-CD2-MOU-Signed.aspx*, accessed September 17, 2015.

55. "WP1: Technical Information Sharing," MN CD2 – Cyber Defence Capability Development official website, June 11, 2015, available from *https://mncd2.ncia.nato.int/ourwork/Pages/WP1-Technical-Information-Sharing.aspx,* accessed September 17, 2015. Per the website, the relevance of this program to NATO operations is:

> The objective of this work package is to deliver a capability [sic] for the efficient exchange of unclassified, but potentially sensitive, cyber defence technical information related to incidents, threats and vulnerabilities amongst national Computer Security Incident Response Teams (CSIRTs).The project enables the participating Nations to build on previous NATO work in the development of national capabilities. The development of this capability through a multinational project has reduced its overall cost per nation.

56. ”WP2: Cyber Defence Situational Awareness,” MN CD2 – Cyber Defence Capability Development official website, May 1, 2015, available from *https://mncd2.ncia.nato.int/ourwork/Pages/WP2-Cyber-Defence-Situational-Awareness.aspx,* accessed September 17, 2015. Per the website, the relevance of this program to NATO operations is:

> The objective of this project is to support nations in developing a CDSA capability. In this projetct [sic], we will: identify requirements and use cases; hold a CDSA solutions conference to assess the market against selected CDSA use cases; demonstrate one or more solutions executing the selected use cases in a high-fidelity environment; and, optionally assist nations in the procurement, deployment, and acceptance testing of the solution in national environments. The purpose of the demonstrations is to verify the degree to which the [selected] solutions would meet operational scenarios. As a minimum, one of the demonstrated CDSA software solutions will be freely deployable for operational use. For all [demonstrations], the aim [is] for the delivered demonstration system to be available for further testing for at least one year.

57. “WP3: Distributed Multi-sensor Collection and Correlation Infrastructure,” MN CD2 – Cyber Defence Capability Development official website, June 11, 2015, available from *https://mncd2.ncia.nato.int/ourwork/Pages/WP3-DMCCI.aspx*, accessed September 17, 2015. Per the website, the Distributed Multi-sensor Collection and Correlation Infrastructure (DMCCI) program was concluded in June 2014; its relevance of this program to NATO operations is:

> The objective of this project was a feasibility study towards the Distributed Multisource Collection and Correlation Infrastructure (DMCCI). The outcome of the study has been positive, DDMCCI [sic] capability development is considered viable, as is its ability to successfully detect the Advanced Persistent Threat (APT). [The] implementation and depoloyment [sic] of the capability is currently being pursued through a follow-on project within the MN CD2 framework, with focus on the Parsing, Correlation and Storage module of DMCCI.

58. "CIICS Enhancements," MN CD2 – Cyber Defence Capability Development official website, June 11, 2015, available from *https://mncd2.ncia.nato.int/ourwork/Pages/WP-4.aspx*, accessed September 17, 2015. Per the website, the relevance of this program to NATO operations is:

> The Work Package provides a vehicle under which enhancements to the Cyber Information and Incident Coordination System (CIICS) can take place. CIICS scope under Work Package (WP) 1 of MN CD2 included implementation for a subset of Low Level Requirements (LLRs) desired by the sponsoring nations. This WP completes fulfilment of all LLRs.

59. "MN CD2 Nations agree to two new Work Packages," MN CD2 – Cyber Defence Capability Development official website, August 10, 2013, available from *https://mncd2.ncia.nato.int/news/Pages/MN-CD2-Board-Meeting-08.aspx*, accessed September 17, 2015. The two new work packages aim to accomplish the following:

> The CIICS Support Work Package will enable the NCI Agency to operate and maintain the NATO CIICS Federation on behalf of participating Nations. The CSAT Work Package will fully explore the feasibility and costs associated with developing a CSAT as a multinational project through a CSAT Continual Operational Readiness Environment (CSAT CORE) – a central, multinational "skeleton" cyber security assessment capability.

60. "Multinational Cyber Defence Education & Training: PoW and State of Play," Overview Brief, Lisbon, Portugal: NATO Emerging Security Challenges Division Science for Peace and Security (SPS) Programme Information Day, October 20, 2014, available from *nato.int/nato_static_fl2014/assets/pdf/pdf_2014_10/20141029_141020-8_Nunes.pdf*, accessed September 17, 2015. The countries with Formal Statements of Interest in the Multinational Cyber Defence Education and Training (MN CD E&T) program at the time of this brief were: Albania, Belgium, Bulgaria, France, Germany, Poland, Portugal, Romania, Spain, Turkey, and the United Kingdom; interested countries were: Czech Republic, Denmark, Estonia, Greece, Hungary, Italy, Latvia, Lithuania, Netherlands, Norway, and Slovenia. The

program's objective is "To fulfill Nations' and NATO's CD E&T shortfalls identified in the GAP analysis that will be performed in cooperation with ACT, in order to support Nations and NATO to comply with NDPP Capability Targets."(slide 3)

61. "Connected Forces Initiative," NATO official website, last updated August 31, 2015, available from *nato.int/cps/en/natohq/topics_98527.htm*, accessed on September 14, 2015.

62. "Wales Summit Declaration," p. 15. para. 68 of the declaration describes the six major parts of the CFI:

> We continue to build on the experience gained in recent operations and improve our interoperability through the Connected Forces Initiative (CFI). Today we have endorsed a substantial CFI Package consisting of six key deliverables, including the high-visibility exercise Trident Juncture 2015, with 25,000 personnel to be hosted by Spain, Portugal, and Italy; a broader and more demanding exercise programme from 2016 onwards; and a deployable Special Operations Component Command headquarters. As a key component in delivering NATO Forces 2020, the CFI addresses the full range of missions, including the most demanding, thereby demonstrating the continued cohesion and resolve of the Alliance. It provides the structure for Allies to train and exercise coherently; reinforces full-spectrum joint and combined training; promotes interoperability, including with partners; and leverages advances in technology, such as the Federated Mission Networking framework, which will enhance information sharing in the Alliance and with partners in support of training, exercises and operations.

63. H. Todd Waller and Joel Gourio, "7 Stepping Stones for Trident Exercises Cyber Defence Transformation," *The Three Swords: The Magazine of the Joint Warfare Centre*, No. 26, May 2014, pp. 40-42. On page 40, the author notes: "Given the importance of cyber defence (CD) to the Alliance, an appreciation of the cyber lessons of STEADFAST (the predecessor to TRIDENT) is essential for achieving a higher level of CD across Alliance operations."

64. "Allied Command Transformation," NATO official website, last updated November 11, 2014, available from *nato.int/cps/en/natohq/topics_52092.htm*, accessed on September 16, 2015.

Allied Command Transformation (ACT) was created in the post-9/11 environment:

> ACT was created as part of a reorganisation of the NATO Command Structure in 2002. This was the first time in NATO's history that a strategic command was solely dedicated to 'transformation,' demonstrating the importance placed by Allies on the roles of transformation and development as continuous and essential drivers for change that will ensure the relevance of the Alliance in a rapidly evolving global security environment.
>
> ACT is organised around four principal functions:
> - strategic thinking;
> - the development of capabilities;
> - education, training and exercises; and
> - cooperation and engagement.

65. "Centre is the first International Military Organization hosted by Estonia," NATO Cooperative Cyber Defence Centre of Excellence, October 28, 2008, available from *https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html*, accessed August 9, 2015. The article noted the significance of the Cooperative Cyber Defence Center of Excellence (CCD COE) being located in the small country of Estonia:

> CCD COE (Cooperative Cyber Defence Centre of Excellence) was activated as an International Military Organization by the decision of the North-Atlantic Council, making it the first IMO hosted by Estonia.
>
> The North-Atlantic Council made the final decision for giving the Cooperative Cyber Defence Centre of Excellence full accreditation and International Military Organizaton status. Such status is nominated according to the Paris Protocol agreement to international military headquarters or other entities by the decision of the North-Atlantic Council. CCD COE is the first organization located in Estonia to have such a status.
>
> 'Estonia has shown that it is not the matter of the size of the defence forces, but the level of special capabilities, that shows their role in enhancing NATO's defencive capabili-

> ties. We appreciate Estonians initiative in the field of cyber defence,' was stated by the NATO ACT Assistant Chief of Staff C4I (Command, Control, Communications, Computers and Intelligence) Major General Koenraad Gijsbergs.

66. "CCD COE – Events," NATO Cooperative Cyber Defence Centre of Excellence, available from *https://ccdcoe.org/events.html*, accessed on September 27, 2015. This webpage includes links to: Cyber Defence Exercises; Cyber Defence Workshops; Cyber Security Conference; Technical Courses; Law Courses; Cyber Defence at Operational Level Course; Awareness e-Course; and Training Courses by Other Entities. The center's stated mission and vision are:

> Our mission is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation
>
> Our vision is to be the main source of expertise in the field of cooperative cyber defence by accumulating, creating, and disseminating knowledge in related matters within NATO, NATO nations and partners.

67. *NATO Accredited Centres Of Excellence 2015*, Norfolk, VA: Allied Command Transformation, 2015, p. 15.

> The Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) is the pre-eminent, independent, multinational source of innovative advice and expertise on all aspects of maritime operations, charged with developing and promoting maritime concepts and doctrine in order for NATO, Sponsoring Nations, Allies and other international partners and organizations to effectively counter current and emerging global maritime security challenges.

68. See Ricky McIver, "Delivering Maritime Security in Global Partnership: Energy and Cyber Security Challenges in the Maritime Domain," Norfolk, VA: Combined Joint Operations from the Sea Centre of Excellence, May 5, 2014, available from *cjoscoe.org/images/Delivering_Maritime_Security_in_Global_Partnership_5_May_14.pdf*, accessed September 25, 2015. See also Kelly A. Mosteller, "Legal questions arising from maritime security considerations in the energy and cyber domains," Norfolk, VA: Com-

bined Joint Operations from the Sea Centre of Excellence, June 2014, available from *cjoscoe.org/images/Legal_Questions_-_Edit.pdf*, accessed September 25, 2015.

69. *NATO Accredited Centres Of Excellence 2015,* pp. 21-22. Also see the website of the Centre of Excellence Defence Against Terrorism (COE-DAT), available from *www.coedat.nato.int/index.html,* accessed September 27, 2015.

70. *Countering Cyber Terrorism Course Report*, Ankara, Turkey: Centre of Excellence Defence Against Terrorism, November 2006, available from *www.coedat.nato.int/publication/course_reports/06-CCT.pdf,* accessed August 9, 2015. In his opening remarks for the course, the Centre of Excellence Defence Against Terrorism (COE-DAT) commander noted the following:

> The topic of 'Cyber Terrorism' as an emerging threat is of great importance, and we hope that this week will increase all of our understanding as to the nature and severity of the threat, and what we can do to reduce this threat. The Internet is an international phenomenon, and any response to Cyber Terrorism will be most effective at the international level. This course can only contribute to our communal response to the threat, and the COE-DAT hopes to identify further areas of research during the planned Advanced Research Workshop in 'Countering Cyber Terrorism' next year. (pp. 2-3)

71. *Terrorist Use of Cyberspace Course Report*, Ankara, Turkey: Centre of Excellence Defence Against Terrorism, May 2014, available from *www.coedat.nato.int/publication/course_reports/11-Terrorist_Use_of_Cyberspace.pdf,* accessed August 9, 2015. The report included an overview of the goals and scope of the course:

> The aim of the course was to emphasize the effects and role of media, especially social media, as a strategic communications for terrorist activities; to prospect, list, and analyze the current cyberterrorism threats, and comprehend their specificity in order to raise awareness of the cyber risks; to discuss proposals of how specific legal issues might be overcome and addressed; to comprehend politics of cybersecurity at global, regional and national levels; and to facilitate understanding among the participants of why international

> cooperation is an essential starter in addressing the challenges that come from terrorist use of cyberspace.
>
> The course was successfully completed accordingly to the agenda. Eleven lecturers from six countries and 66 attendees from 23 countries participated in the course, representing military institutions, law enforcement agencies, government departments and academia. There were 16 lectures, two working group preparation sessions, two working group presentations and one panel discussion held throughout the course. (p. 3)

72. *Critical Infrastructure Protection against Terrorist Attacks*, Ankara, Turkey: Centre of Excellence Defence Against Terrorism, November 2014, available from *www.coedat.nato.int/publication/course_reports/12-CIP.pdf,* accessed September 27, 2015. In the section on "Issues and Concerns," the report included:

> For Alliance members, cyber threats targeted at security network is one of the most serious economic and national security challenges they face. NATO has prepared a 'Strategic Concept' in 2010, and revised it in 2011, to further develop its ability to prevent, detect, defend against and recover from cyber-attacks by expanding its capacity in cybersecurity. NATO Member States reinforced the importance of international cooperation in the Chicago Summit Declaration of May 2012. Cooperation between member states is important for organizing, creating and enforcing a security standard about those national cyber-systems, which are vital for the effective functioning of the whole alliance. This includes collaboration on a number of fronts including optimized information sharing, situational awareness, and secure interoperability based on agreed sets of common standards. Countering terrorism and the protection of CI requires partnerships. Achieving NATO counter-terrorism goals requires an integrated, collaborative approach by government, the private sector, citizens, and other international partners. It will never be possible to stop all terrorist attacks. (p. 16)

73. Allied Joint Publication (AJP)-01(D), *Allied Joint Doctrine*, Brussels, Belgium: NATO Standardization Office, December 2010, available from *nso.nato.int/nso/zpublic/ap/ajp-01(d).pdf*, ac-

cessed September 28, 2015. Per paragraph 0509 (p. 5-2), the focus of military operations aspect remains focused on information operations, of which cyber is a subset, as one of the seven principal joint functions for a commander to utilize (the others are Manoeuvre and Fires; Command and Control; Intelligence; Sustainability; Force Protections; and Civil Military Co-operation). The following are cyberspace-related excerpts from the document:

> The security challenges now facing NATO, which extend beyond its traditional area of responsibility, include areas such as missile defence and cyber-operations. (p. 2-1, para. 0203)
>
> In addition, the Alliance's growing reliance on information and information systems creates vulnerability to cyber attack, which may reduce or cancel NATO's superiority in conventional weaponry. (p. 2-3, para. 0210)
>
> One of the key contemporary challenges within the realms of protection is defensive information operations, specifically cyber, communications and command and control systems' protections. This is an area of increasing vulnerability, directly proportional to NATO's levels of dependence on such systems. (p. 5-14, para. 0533)

74. Allied Joint Publication (AJP)-6, *Allied Joint Doctrine for Communication and Information Systems*, Brussels, Belgium: NATO Standardization Office, April 6, 2011, available from *nso.nato.int/nso/zPublic/ap/ajp-6.pdf*, accessed September 27, 2015. Information assurance is comprised of the five pillars of availability, integrity, authentication, confidentiality, and non-repudiation of information; activities related to these pillars are described as:

> Information assurance requires management processes to ensure the systems and networks employed to manage the critical information used by an organization are reliable and secure, and processes are in place to detect and counter malicious activity. Information assurance includes elements of physical security, such as personnel and document security, and information security. This includes a range of electronic techniques such as communications security (COMSEC), incorporating emission control (EMCON) and emission security, computer security (COMPUSEC), transmission security, defensive monitoring and technical inspection tech-

> niques, counter-eavesdropping, limited electronic sweeps, and vulnerability analysis. COMSEC and COMPUSEC are integral elements of all military CIS operations and must be considered throughout planning and execution. Information must be protected at the correct level, ensuring that valid information is available to authorized users, and preventing valid information from being available to unauthorized persons. The degree of security provided must be consistent with the requirements of CIS users, the vulnerability of transmission media to interception and exploitation, and the reliability and releasability of COMSEC hardware and software.4 Information assurance is the protection and defence of information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. (p. 1-4, para. 0103.f.)

75. Allied Joint Publication (AJP)-5, *Allied Joint Doctrine for Operational-Level Planning*, Brussels, Belgium: NATO Standardization Office, June 2013, available from *nso.nato.int/nso/zpublic/ap/ajp-5%20e.pdf*, accessed September 27, 2015. The connection of defensive cyber operations to joint targeting and joint fires is detailed on p. 3-49, para. 0379.c.(9). Placing cyberspace amongst the traditional military domains is stated as:

> Functional Planning Guides provide planning guidance in specific functional areas. Functional areas include warfare areas that are normally divided into components such as maritime, air, space, cyberspace and land. (p. 1-12, para. 0114.b.(3))

76. Allied Joint Publication (AJP)-3(B), *Allied Joint Doctrine for the Conduct of Operations*, Brussels, Belgium: NATO Standardization Office, March 2011, available from *nso.nato.int/nso/zpublic/ap/ajp-3(b).pdf*, accessed September 27, 2015, p. 1-8 (para. 128). The placement of cyberspace in the information environment is stated on p. ix:

> This AJP describes the fundamental operational aspects of joint operations and provides guidance on the conduct of joint operations at the operational level. These operations are complex and contain all the different tasks that span the range of military operations, from humanitarian assistance to combat. Most operations will take place in all environments (maritime, land, air and space, information including

> cyberspace) while some will predominantly favour a single one, such as maritime.

77. *Ibid*., p. 1-26. The Joint Force Commander's establishing directive is described in para. 192:

> These directives are essentially an order that specifies the purpose of the support relationship, the effect desired and the scope of action to be taken and should include, but is not limited to the following:
>
> f. Establishment of air, sea, and ground manoeuvre control measures and cyberspace operations protocols.

78. *Ibid*., p. 4-3. Para. 0410 clearly implies that cyberspace is part of the information environment:

> The operating environment includes the sea, land, air and space the adversary, neutral and friendly actors, facilities, weather, terrain, electromagnetic spectrum (EMS), and the information environment, which includes cyberspace, within the JOA and areas of interest.

79. Hutson, p. 36. The author notes some current inconsistency with regard to NATO cyber defense (CD) doctrine:

> There is little to no NATO CD specific doctrine, much less agreed cyber related definitions or taxonomy for cyber for the deployed Commander. This lack of doctrine, however, is made more problematic by the fact that there is approved NATO Doctrine for Computer Network Operations (CNO) and Computer Network Defence (CND) in the context of Information Operations Doctrine (AJP 3.10), and for Information Assurance within the context of the AJP-6 series - both of which are not always consistent with approved NATO CD policy and developing NATO cyber taxonomy.

80. *Ibid*., p. 39.

81. *Ibid*., p. 37.

82. See the "About" page, "NATO Communications and Information Agency," NCI Agency official website.

83. "NATO launches Industry Cyber Partnership," NATO News official website, last updated September 17, 2014, available from *nato.int/cps/en/natolive/news_113121.htm?selectedLocale=en*, accessed September 17, 2015.

84. "Our objectives and principles," NATO Industry Cyber Partnership official website, available from *www.nicp.nato.int/objectives-and-principles/index.html,* accessed September 17, 2015. The specific objectives of the NICP are listed as:

> As part of NATO's efforts to strengthen its cyber defence, the NATO Industry Cyber Partnership will have the following objectives:
>
> - Improve cyber defence in NATO's defence supply chain;
> - Facilitate participation of industry in multinational Smart Defence projects;
> - Contribute to the Alliance's efforts in cyber defence education, training and exercises;
> - Improve sharing of best practices and expertise on preparedness and recovery (to include technology trends);
> - Build on existing NATO initiatives for industry engagement, providing specific focus and coherence on the cyber aspects;
> - Improve sharing of expertise, information and experience of operating under the constant threat of cyber attack, including information on threats and vulnerabilities, e.g. malware information sharing;
> - Help NATO and Allies to learn from industry;
> - Facilitate access by Allies to a network of trusted industry/enterprises;
> - Raise awareness and improve the understanding of cyber risks;
> - Help build access and trust between NATO and the private sector;
> - Leverage private sector developments for capability development, and;
> - Generate efficient and adequate support in case of cyber incidents.

85. *Industry Cyber Security Information Sharing at the Technical Level Guidelines Revision 1*, Brussels, Belgium: NATO Communication and Information Agency, March 28, 2014. The Introduction section (p. 1) of these guidelines outlines the motivation for creating an effective working relationship:

> NATO and industry working with NATO continue to face increasing risks that Information exchanged or stored on their networks and systems can be accessed, affected or infected through malicious cyber acts thereby causing damage to the Alliance and its Members. NATO and industry need to be able to prevent and counter such threats and to analyse and share data in order to understand the nature, extent and possible sources of such incidents and to react to threats.
>
> The NATO Communications and Information Agency (NCI Agency) is responsible for identifying and promoting the development of essential capabilities that meet NATO's and its Member Nations' needs in ensuring cyber safety and security. NATO capabilities to identify, prevent, detect and respond to external threats to NATO CIS infrastructure are primarily performed by the NCI Agency NATO Computer Incident Response Capability Technical Centre (NCIRC TC).
>
> With these Guidelines, the NCI Agency implements a voluntary bilateral Cyber Information Sharing Programme which will allow industry working with NATO and NATO to share cyber security Information in order to mutually enhance situational awareness and the protection of their networks and systems.

86. "NCI Agency Pilot Project Reveals Key Lesson on Strengthening NATO Cyber Defence," NATO Industry Cyber Partnership official website, September 9, 2015, available from *ncia.nato.int/NewsRoom/Pages/150909-Cyber-Incubator.aspx*, accessed September 17, 2015. The article included a summary of the goals of the Cyber Security Incubator Pilot Project:

> The NCI Agency developed the cyber security incubator concept with the aim of exploring a new model for cooperation between NATO and industry partners that could decrease the time to develop responses to NATO's cyber security challenges. The incubator pilot project identified an

approach to bring rapid results from academia and industry to NATO, and discussions are underway to determine how this framework could be extended to integrate these ideas into NATO's IT environment in a timeframe that keeps pace with evolving cyber threats. This is likely to be the target of a second stage of the incubator. (p. 2)

87. "NCI Agency and Microsoft sign cyber cooperation agreement," NATO Industry Cyber Partnership official website, September 14, 2015, available from *ncia.nato.int/NewsRoom/Pages/150914-NCIAgency-Microsoft-GSP.aspx,* accessed on September 17, 2015. The agreement also includes details regarding intelligence sharing:

> The agreement expands technical information sharing between Microsoft, other GSP parties and the NCI Agency. The NCI Agency will gain access to technical information, and documentation about Microsoft products and services, as well as information about internet safety, threat intelligence, online training tools and guidance to help mitigate the effects of cyberattacks across the region. A practical effect will be, for instance that Microsoft will provide the Agency with data about hosts that have been infected with botnet exploits, and the Agency will be able use this data to identify and remediate potential vulnerabilities in these systems. (p. 1)

88. Siw Tynes Johnsen, "Norway co-leading the multi-national project on cyber defence and operational planning," *The Three Swords: The Magazine of the Joint Warfare Centre*, No. 26, May 2014, pp. 46-47.

89. Multinational Capability Development Campaign, *MCDC 2013-2014 Catalog of Products*, All Partners Access Network, p. 2, available from *https://wss.apan.org/s/MEpub/default.aspx*, accessed September 15, 2015. The expected outcomes of MCDC 2013-2014 are summarized as:

> MCDC 2013-2014 Focus Area results described in this summary have the potential to significantly enhance both coalition and national operating capabilities while narrowing known gaps. This latest campaign served to increase collective understanding within each of the separate domains and

> provided the opportunity to further explore the nature of their interconnectedness. The products developed provide a common foundation for national and organizational capability development in the areas of doctrine, organization, training, materiel, leadership education, personnel, facilities, and policy. (p. i)

90. *Ibid.,* p. 2. The other six Focus Areas of the projects were: Combined Operational Fires; Combined Operations from the Sea Through the Littoral; Maritime Approach to Combined Operational Access; Role of Autonomous Systems in Gaining Operational Access; Strategic Communication in Combined Operational Access–Information Activities and Emerging Communication Practices; and Understand to Prevent. Contributing countries to the Cyber Implications for Combined Operational Access (CICOA) work were: Austria, Canada, Finland, Hungary, Netherlands, Poland, Spain, Sweden, Switzerland, and U.K. as well as organizations of the European Union and NATO ACT. The CICOA problem statement was:

> This Focus Area will seek to continue these efforts by working to integrate cyber into the multinational planning processes. Operational planning requires an understanding of cyberspace, however planners, and commanders, do not have clear cyber situational awareness. In spite of the importance of cyber aspects for combined joint operational access, they are not addressed in the multinational operations planning processes, such as the COPD. The integration of cyber into the planning process can be supported by procedural and technical capabilities/solutions in order to facilitate the commander's assessment. (p. 11)

91. *Ibid.,* pp. 12-14.

92. Multinational Capability Development Campaign, *MCDC 2015-16 Information Paper*, July 6, 2015, available from https://wss.apan.org/s/MCDCpub/MCDC_2015_16/default.aspx, accessed September 28, 2015. Participating countries for the MDCO are: Austria, Canada, Finland, Hungary, Netherlands, Norway, Poland, Spain, Sweden, Switzerland, and U.K. as well as organizations of the European Union and NATO ACT. Also, Denmark, Germany, and Japan are observers.

93. "Rome Atlantic Forum – 'NATO and the Future of Cyber Security'," NATO Defense College website, December 2, 2013, available from *www.ndc.nato.int/news/news.php?icode=612*, accessed September 29, 2015. The purpose of the forum was summarized as:

> The aim of this event was to promote discussion and research on a security issue relevant not only to NATO, but to the international security community as a whole: cyber security, and NATO's approach to dealing with cyber threats. As stressed by the IAC [Italian Atlantic Committee] and the ATA [Atlantic Treaty Association]: 'Among the emerging threats to security, the cyber one has taken an increasing relevance due to its potential impact on government and institutional apparatuses, the industrial system and communications, as well as the welfare of the citizens of modern interconnected societies. While critical infrastructure protection is a national responsibility, NATO represents an added value in strengthening the prevention, resilience and response capabilities of the member States.' In this respect, the Rome Atlantic Forum marks an important step forward towards greater awareness of a particularly topical security concern.

94. The following papers from the NATO Defense College Research Division are available for download in pdf format available from *www.ndc.nato.int/research/research.php?icode=3:* Christine Hegenbart, *Semantics Matter: NATO, Cyberspace and Future Threats*, July 2014; Vincent Joubert, *Five years after Estonia's cyber attacks: lessons learned for NATO?* May 2012; and Jeffrey Hunker, *Cyber war and cyber power: Issues for NATO doctrine*, November 2010.

95. "NATO School Oberammergau-Academics," official website, available from *www.natoschool.nato.int/Academics,* accessed September 29, 2015. The school's six resident courses on cyber and information operations are:

N3-16:	NATO Senior Officer Information Operations Course
N3-19:	NATO Information Operations Course
M6-108:	Network Security Course
M6-109:	Network Vulnerability Assessment Course
M6-110:	Cyber Incident Handling & Disaster Recovery Course
M6-111:	Network Traffic Analysis

96. Waller, "Cyberspace Implications for NATO Operations," p. 24. In this article, the author describes "a blueprint for Joint Warfare Centre support to NATO cyber defence" to support the centre's vision:

> The Joint Warfare Centre vision is to provide the best training support possible for the collective training and certification of NATO's joint operational and component level Headquarters. Now that cyber defence is becoming a more important aspect of operational readiness, the JWC is beginning to generate training consistent with this emerging requirement. Like any new requirement, especially one as broad and unique as conducting operations in a cyber-contested environment, multiple steps are necessary to achieve a robust capability.

97. "Courses-Course Descriptions," NATO Communications and Information Systems School website, available from *www.nciss.nato.int/courses_description.php,* accessed September 28, 2015. Per its website, the NCISS mission is:

> The NCISS is embedded in the NCI Agency's Education & Training (E&T) Service Line (SL) for training delivery and provides cost-effective high quality formal individual training to personnel assigned to both NATO Command Structure (NCS) and NATO Force Structure (NFS), the Alliance Nations, PfP and other organisations for the effective and efficient management, control, administration, operation and maintenance of NATO assigned Communications and Information Systems (CIS) as well as for defined Functional Services (FS)/Functional Area Services (FAS).
>
> The cyber-related courses currently offered by the NCISS are:
>
> 006: Cyber Defence – Crypto Administration and CARDS for NATO Custodians and Alternates
> 067: Cyber Defence – COMSEC System Engineering
> 233: Cyber Defence – DEKMS (DACAN Electronic Key Management System)
> 279: Cyber Defence – COMPUSEC Practitioners
> 280: Cyber Defence – INFOSEC Officer

98. Piret Pernik, "Increasing NATO's Role in Cyber Defence," International Centre for Defence and Security, Estonia, Blog, Cyber Security, August 28, 2014, available from *icds.ee/blog/article/increasing-natos-role-in-cyber-defence/*, accessed on September 16, 2015. The author notes:

> The training field enables Allies to test and exercise their cyber capabilities within a NATO structure, to feed lessons learned and new concepts into the Alliance; and to ensure that cyber experts across the Alliance share the same levels of expertise.

99. Ali, pp. 33-34.

100. "Largest ever NATO cyber defence exercise gets underway," NATO News official website, November 18, 2014, available from *nato.int/cps/en/natohq/news_114902.htm*, accessed September 17, 2015.

101. Rick McCartney, "Exercise Cyber Coalition 2014," NCI Agency official website, November 26, 2014, available from *ncia.nato.int/NewsRoom/Pages/141126-cyber-coalition.aspx*, accessed September 28, 2015. The article noted the ambitious scope of the exercise:

> While this was a cyber defence exercise, the objectives went far beyond cyber security and technical capability challenges. Especially important was the exercising of communication between various NATO bodies, national cyber defence capabilities, and industry partners. This year's exercise scenarios included malicious code, mobile device eavesdropping, loss of precision radar targeting capabilities, and hostile intelligence service agents acting from inside the coalition network. As a response to one of the exercise injects, the newly acquired Cyber Security Rapid Reaction Team deployed with a full complement of field-hardened equipment to Athens, Greece, demonstrating its ability to be on site on short notice to diagnose cyber security issues and swiftly restore operational capability.

102. *Ibid*.

103. "Nato starts Cyber Coalition 2013 exercise," army-technology.com website, November 28, 2013, available from *army-technology.com/news/newsnato-starts-cyber-coalition-2013*, accessed on September 28, 2015.

104. "NATO conducts annual crisis management exercise (CMX) and cyber coalition exercise," NATO Press Release (2012)131, North Atlantic Treaty Organization, October 31, 2012, available from *nato.int/cps/en/natolive/news_91115.htm?mode=pressrelease*, accessed September 28, 2015. The exercise scenario is summarized as:

> The two exercises CMX 12 and Cyber Coalition 12 will be conducted based on one single fictitious scenario portraying an escalating threat from chemical, biological and radiological attacks, including large scale cyber attacks affecting NATO and national critical infrastructure. This exercise scenario will require Allied political direction taking into account the advice of NATO military authorities and technical cyber defence bodies on possible measures to handle asymmetric threats.

105. "Cyber Defence Exercises / Locked Shields 2015," NATO Cooperative Cyber Defence Centre of Excellence, April 20, 2015, available from *https://ccdcoe.org/locked-shields-2015.html*, accessed September 9, 2015. Specific details of the exercise include:

> The largest of its kind globally, Locked Shields is unique in using realistic technologies, networks and attack methods. In 2015, new attack vectors included ICS/SCADA [Industrial Control Systems/Supervisory Control and Data Acquisition] systems and Windows 8 and 10 operating systems, as well as an element of active defence. In addition to technical and forensic challenges, Locked Shields also includes media and legal injects. It thus provides insight into how complex a modern cyber defence crisis can be, and what is required from nations in order to be able to cope with these threats.

106. Liis Kangsepp, "In NATO Cyber Wargame, Berlya Fends Off Arch Enemy Crimsonia," *The Wall Street Journal*, April 24, 2015, available from *blogs.wsj.com/digits/2015/04/24/in-nato-cyber-wargame-berlya-fends-off-arch-enemy-crimsonia/tab/print/*, accessed August 25, 2015.

107. To view the After Action Reports from the Locked Shields cyber exercises, see the NATO Cooperative Cyber Defence Centre of Excellence website, available from *https://ccdcoe.org/event/cyber-defence-exercises.html*.

108. H. Todd Waller, "The Joint Warfare Centre launches cyber defence training with STEADFAST JUNCTURE 2011," *The Three Swords: The Magazine of the Joint Warfare Centre,* No. 21, Autumn/Winter 2011, p. 46. The exercise was successful in raising awareness of operational cyber issues amongst the battlestaff:

> Consequently, the battlestaff responded to a number of cyber injects that were both direct and subtle, and also began to ask some very good questions about how cyber threats could be treated more thoroughly in the planning process to either mitigate or avoid their effects. The battlestaff also had the opportunity to experience how cyber attacks against host nation critical infrastructures could impact operations and the stability of the government. With this understanding came new insights into how the command might assess its vulnerabilities during the planning phase for a future contingency operation or exercise. (pp. 46-47)

109. *Ibid*., p. 46.

110. Hutson, p. 39. The author describes the cyber attacks that occurred during Steadfast Jazz 2013 (SFJZ 13):

> NATO soldiers were deployed in multiple forward locations, with the JTF Headquarters located just outside of Riga. During SFJZ 13, Baltic media and defence officials reported a growing number of cyber-attacks against state administration, defence, and private sector homepages. False messages were posted on the attacked websites saying that the security parameters of the website did not comply with the requirements of the CCD COE. Personnel in the Baltic and Polish defence sectors received fake emails in the name of the CCD COE. The Latvian News Agency reported that a hacker group 'Anonymous Ukraine' was behind the cyber-attacks; and partly as a consequence to these events, the Latvian Defence Minister emphasised the importance of Latvia's investment in a cyber defence unit for its Latvian Home Guard.

111. "NATO Allies testing operational capabilities during the 2014 CWIX," NATO Joint Force Training Centre website, available from *www.jftc.nato.int/cwix-2014/organization/hq-jftc/the-2014-cwix-at-jftc,* accessed September 17, 2015. The description of 2014 CWIX included connections to NATO operational initiatives:

> As one of NATO's foundation venues for achieving and demonstrating interoperability, CWIX is fully in line with ACT's Smart Defence concept and the Connected Forces Initiative (CFI). NATO and its member nations can pool and share resources to achieve interoperability before deployment and collaborate on future initiatives, including Federated Mission Networking (FMN), Cyber Defence and Communication and Information Systems (CIS) capability development.

112. "Final Preparations for Exercise Trident Juncture 2015," Allied Joint Force Command Brunssum website, September 11, 2015, available from *jfcbs.nato.int/page7715057/final-preparations-for-exercise-trident-juncture-2015.aspx,* accessed September 29, 2015.

113. "Exercise Trident Juncture 2015 Academics," NATO Allied Command Operations website, January 16, 2015, available from *aco.nato.int/exercise-trident-juncture-2015-academics.aspx*, accessed September 29, 2015. The myriad goals of Trident Juncture 2015 exercise (TRJE15) are summarized in the article as:

> The purpose of TRJE15 is to train and test the NATO Response Force, a high readiness and technologically advanced force comprising of land, air, maritime and special forces units capable of being deployed quickly on operations wherever needed. The exercise represents the final step in the certification process for the command and control elements of the NRF for 2016 where JFC Brunssum will be the on-call Standby Command. The exercise will also allow Allies and partners the occasion to train, deploy and exercise in a complex and distributed environment.

114. Waller and Gourio, "7 Stepping Stones," pp. 40-42. In summary, the topics comprising the "7 Stepping Stones" are:

1. CD [cyber defence] is much more than a technical issue
2. Operational level cyber defence is emerging and needs nurturing
3. Cyber defence SMEs [subject matter experts] are the key to A+ performance
4. WANTED! Comprehensive cyber defence education and training
5. Empower cyber defence during Crisis Response Planning (CRP)
6. Create a playbook for all cyber defence-related exercises
7. Achieve more realistic CD training without excessive risk

115. James A. Lewis, *The Role of Offensive Cyber Operations in NATO's Collective Defense*, Tallinn Paper No. 8, Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2015, p. 2, available from *https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf*, accessed on August 25, 2015. At the time of publication, Mr. Lewis was the Director and Senior Fellow, Strategic Technologies Program, Center for Strategic and International Studies.

116. *Ibid.,* p. 7. The author notes that:

> Some level of cyber capability is being acquired by all advanced militaries, and perhaps a dozen countries can be identified from public sources as procuring offensive cyber capabilities. These countries include several NATO members.
> As with nuclear weapons, the capability to undertake offensive cyber operations is a club within a club in NATO, with largely the same membership – the US, the UK and France. Germany's armed forces may also be developing offensive cyber capabilities.

117. Joint Chiefs of Staff, Joint Publication 3-12 (R), *Cyberspace Operations*, Washington, DC: Joint Chiefs of Staff, original release February 5, 2013 updated as unclassified public document on October 21, 2014. In Chapter 2, the description of Military Operations In and Through Cyberspace includes in paragraph 2.a.(1):

> **Offensive Cyberspace Operations.** OCO are CO intended to project power by the application of force in and through

> cyberspace. OCO will be authorized like offensive operations in the physical domains, via an execute order (EXORD). OCO requires deconfliction in accordance with (IAW) current policies. (p. II-2)

118. Florian De Castro, "A Call for NATO to Operationalize Cyberspace," *The Three Swords: The Magazine of the Joint Warfare Centre*, No. 26, May 2014, pp. 45. The author went on to note the connection between active cyber defense and offensive cyber:

> NATO must realise that the offensive capability of cyber surpasses any defensive capability that can be implemented. The area that needs to be defended is so vast that it does not matter how 'resilient' the cyber network is. NATO will not be able to 'deter' the most determined adversaries without an offensive capability. The military analogy is that NATO has built the equivalent of a Cyber Maginot Line against a Cyber Blitzkrieg. One should not infer that the Maginot Line is not needed, but that the Blitzkrieg is equally needed. We must not forget that although NATO is a defensive Alliance, the Alliance possesses equal measure of defensive and offensive capabilities. (pp. 45-46)

119. See Jeffrey L. Caton, "Exploring the Prudent Limits of Automated Cyber Attack," in *Proceeding of 5th International Conference on Cyber Conflict*, Tallinn, Estonia: NATO Cooperative Cyber Defence Center of Excellence and IEEE, June 2013, pp. 145-160.

120. Lewis, p. 9.

121. Healey and Jordan, pp. 6-7.

122. Clorinda Trujillo, "The Limits of Cyberspace Deterrence," *Joint Force Quarterly*, No. 75, 4th Qtr. 2014, pp. 43-52. The author lists several ways of pursuing deterrence in cyberspace:

> Based on this existing policy and doctrine and additional scholarly efforts,
> - proposed cyberspace deterrent options include:
> - develop policy and legal procedures
> - develop other credible response options [including offensive actions in cyberspace]
> - pursue partnerships

- secure cyberspace
- enhance resiliency
- strengthen defense
- conduct cyberspace deception. (p. 47)

123. Jeffrey L. Caton, *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, January 2015.

124. Christine Hegenbart, *Semantics Matter: NATO, Cyberspace and Future Threats*, Rome, Italy: NATO Defense College Research Division, July 2014, p. 9. The author divides the cyber conflict escalation ladder into six rungs of increasing severity: (1) Hacktivism/Cyber Vandalism; (2) Cyber crime; (3) Cyber espionage; (4) Cyber sabotage; (5) Cyber terrorism; and (6) Cyber war.

125. Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington, DC: The White House, May 2011, p. 14.

126. Trujillo, p. 49.

127. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, NY: Cambridge University Press, 2013.

128. Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations*, Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2010, available from *https://ccdcoe.org/publications/books/legalconsiderations.pdf*, accessed September 30, 2015.

129. Ramberto A. Torruella, Jr., "Determining Hostile Intent in Cyberspace," *Joint Force Quarterly*, No. 75, 4th Quarter 2014, pp. 114-121.

130. Enrico Benedetto Cossidente, "Legal Aspects of Cyber and Cyber-Related Issues Affecting NATO," *NATO Legal Gazette*, Issue 75, December 2014, pp. 11-15. Regarding the actions of Russia and China in cyberspace, the author notes:

> NATO's position has to be compared with the actions of non-NATO actors, specifically Russia and China. These two nations have demonstrated mixed behaviors concerning their perception of international law in cyber space. In 2013 a UN Group of Experts, that included representatives of Russia and China, agreed that international law applies to cyber space; however, both Russia and China did not agree to a reference of international humanitarian law (IHL) with regard to cyber activities. Alternately they are holding this position in regard to IHL while promoting the creation of an international treaty on cyber. Though there have been some Russian actions in cyber space there is no clear evidence of Russian State actors' involvement in cyber attacks against Estonia or the US. It is a fact, however, that cyber-attacks were conducted from Russia during its military operations against Georgia. China also has a history of conducting cyber-attacks, but its activities are mainly related to the gathering of military/commercial intelligence. Some of these cyber activities have led to claims being brought against Chinese citizens in US domestic courts. (pp. 14-15)

131. "NATO Cooperative Cyber Defence Centre of Excellence Research," official website, available from *https://ccdcoe.org/research.html,* accessed on September 15, 2015. The website includes a concise description of the scope of the Tallinn Manual and its update:

> The focus of the original Tallinn Manual is on the most disruptive and destructive cyber operations – those that qualify as 'armed attacks' and therefore allow States to respond in self-defence, and those taking place during armed conflict. Since the threat of cyber operations with such consequences is especially alarming to States, most academic research has focused on these issues.
>
> Yet, States are challenged daily by malevolent cyber operations that do not rise to the aforementioned levels. The Tallinn 2.0 project examines the international legal framework that applies to such cyber operations. The relevant legal regimes include the law of State responsibility, the law of the sea, international telecommunications law, space law, diplomatic and consular law, and, with respect to individuals, human rights law. Tallinn 2.0 also explores how the general principles of international law, such as sovereignty, juris-

> diction, due diligence and the prohibition of intervention, apply in the cyber context.

132. "Law Courses/International Law of Cyber Operations," NATO Cooperative Cyber Defence Centre of Excellence website, available from *https://ccdcoe.org/law-course-may.html*, accessed September 30, 2015.

133. Hanneke Piters, "Cyber Warfare and the Concept of Direct Participation in Hostilities," *NATO Legal Gazette*, Issue 75, December 2014, pp. 46-57. The author summarizes the potential legal challenges facing NATO support contractors in his conclusion:

> NATO member countries increasingly employ civilian specialists and outsource tasks to private contractors in the complex cyber domain. The implications for civilian employees and private contractors who are taking a direct part in hostilities can be significant. First, they lose their protection and can be targeted by cyber or other means. Second, they are not included in the proportionality and precautions in attack assessment. Third, they may be held liable and be punished for their actions. Moreover, NATO member countries that let them take a direct part may violate their obligations under international law. Therefore, it is important for legal advisors to know what acts in the cyber domain constitute direct participation in hostilities. This article addresses the three cumulative criteria laid down in the Interpretive Guidance (1) 'threshold of harm,' (2) 'direct causation,' and (3) 'belligerent nexus,' and how they generally apply to the cyber domain and particularly (1) research, designing and writing, (2) installing, service and maintenance, and (3) operation of computer programs. (p. 56)

134. "Lisbon Summit Declaration," pp. 10-11.

135. Piret Pernik, *Improving Cyber Security: NATO and the EU*, Tallinn, Estonia: International Centre for Defence Studies, September 2014, p. 1. The author describes the EU approach to cyber security:

> As a politico-economic union, EU's main areas of responsibility for cyber security concern primary internal security issues - police and criminal justice cooperation in the fight

> against cyber-crime, the protection of critical infrastructures - and international cooperation. Compared to NATO, the EU is a latecomer concerning the national security and defence aspects of cyber security. It identified for the first time only in 2008 cyber threats as a key challenge that, in addition to economic and political, also has a military dimension. Until then it dealt primary with network and information security, cyber-crime; and to a lesser degree with cyber-terrorism, while its approach was fragmented with overlapping parallel policies. (p. 2)

136. See The World in 2020 – Can NATO Protect Us? pp. 25-30, and Smedts, pp. 18-22.

137. Pernik, *Improving Cyber Security*, p. 3.

138. *Ibid.,* pp. 7-9. With regard to differences between the EU and NATO cyber security, the author notes the following:

> Both NATO and the EU stress that cyber security of its member states is a national responsibility. In the EU there is no central authority responsible for common cyber security, while in NATO the top political decision-making body NAC exercises principal decision-making authority and overseas the development on NATO's cyber defence posture. (pp. 7-8)
>
> Another difference lies in the ownership of the networks: NATO 'owns' its command, control, communications, computers, and information systems while the EU does not own ICT infrastructure depending on the member states networks for CSDP missions (Robinson 2013). (p. 8)

139. *EU Cyber Defence Policy Framework*, Outcome of Proceedings document 15585/14, Brussels, Belgium: Council of the European Union, November 18, 2014, available from *europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf*, accessed on August 25, 2015.

140. *Ibid*., pp. 12-13.

141. U.S. Cyber Command Factsheet, U.S. Strategic Command public website, Offutt AFB, NE: U.S. Strategic Command, August

2013, available from *stratcom.mil/factsheets/2/Cyber_Command/*, accessed October 22, 2015. U.S. Cyber Command reached its full operational capability on October 31, 2010. See also, Headquarters, Department of the Army, Establishment of the United States Army Cyber Command, General Order No. 2010-26, Washington, DC: Headquarters, Department of the Army, October 1, 2010.

142. "Defending the networks: The NATO Policy on Cyber Defence"; and *Department of Defense Strategy for Operating in Cyberspace,* Washington DC: Department of Defense, July 2011.

143. "Wales Summit Declaration," para. 72; and *The Department of Defense Cyber Strategy*, Washington DC: Department of Defense, April, 2015.

144. Philip Breedlove, "Statement of General Philip Breedlove, Commander, U.S. Forces Europe, to the House Armed Services Committee," Washington, DC: Government Printing Office, pp. 23-24, available from *eucom.mil/mission/background/posture-statement*, accessed October 22, 2015.

145. Eric A. Brown, "5th Signal Command opens cybercenter," *Stars and Stripes*, July 23, 2014, available from *stripes.com/news/5th-signal-command-opens-cybercenter-1.294824*, accessed October 21, 2015.

146. Breedlove, "Statement of General Philip Breedlove," pp. 23-25.

147. "United States Army Cyber Center of Excellence Strategic Plan," Fort Gordon, GA: U.S. Army Cyber Center of Excellence, September 2015, p. 10, available from *cybercoe.army.mil/images/CyberCoE%20Documents/strategic_plan_2015_revision4_9_14_2015.pdf,* accessed October 22, 2015. The doctrine initiative is under the third of four lines of effort for the Strategic Plan. Description of the initiative is:

> Initiative A: Establish Foundational Doctrine for Army Cyberspace Operations That Is Consistent With Joint Doctrinal Tenets.
> Doctrine provides fundamental principles which guide military actions in support of operational objectives, drives how

Army forces are organized and equipped, and serves as the basis for all Soldier and leader training and education (TR 71-20-3). Field Manual (FM) 3-12 'Cyberspace Operations' will serve as the foundational framework for cyberspace planning, integration and execution. It is intended to supersede FM 3-38, 'Cyber Electromagnetic Activities,' which introduced commanders to cyber terminology and use of allocated staff but failed to address operational principles or outline Army cyberspace operations concepts. As cyberspace operations are inherently joint in nature, it is essential that FM 3-12 and all subsequent doctrinal manuals be consistent with "The U.S. Army Operating Concept," Joint and intelligence community cyberspace principles, standards and common practice to ensure 'interoperability from birth'.

148. William B. King, "US Army Cyber Center of Excellence commander talks cyber with German signal Soldiers," online news article, Wiesbaden, Germany: 5th Signal Command Public Affairs, April 1, 2015, available from *www.army.mil/article/145607/*, accessed October 21, 2015.

149. "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," Washington, DC: Department of Defense, January 2013, p. ii.

150. *Ibid.*, p. 7. Details on the report's first recommendation include:

The [Defense Science Board] Task Force believes that our [U.S.] capacity for deterrence will remain viable into the foreseeable future, only because cyber practitioners that pose Tier V-VI level threats are limited to a few state actors who have much to hold at risk, combined with confidence in our ability to attribute an existential level attack.

151. *Ibid.*, p. 7.

152. *Ibid.*, p. 8. Details on the report's second recommendation include:

To ensure the President has options beyond a nuclear-only response to a catastrophic cyber attack, the DoD must develop a mix of offensive cyber and high-confidence conventional capabilities. Cyber offense may provide the means

to respond in-kind. The protected conventional capability should provide credible and observable kinetic effects globally. Forces supporting this capability are isolated and segmented from general purpose forces to maintain the highest level of cyber resiliency at an affordable cost. Nuclear weapons would remain the ultimate response and anchor the deterrence ladder. This strategy builds a real ladder of capabilities and alleviates the need to protect all of our systems to the highest level requirements, which is unaffordable for the nation. Similar to the prior argument regarding the cyber resiliency of the nuclear deterrent, DoD must ensure that some portion of its conventional capability is able to provide assured operations for theater and regional operations within a full-spectrum, cyber-stressed environment.

153. "The Department of Defense Cyber Strategy," p. 27.

154. "Assuring our allies through investment in Europe's regional cyber, C4 interoperability," U.S. European Command online news article, Stuttgart, Germany: U.S. European Command Cyber Directorate, April 2, 2014, available from *eucom.mil/media-library/article/25642/assuring-our-allies-through-investment-in-europes-regional-cyber-c4-interoperability,* accessed October 22, 2015.

155. William B. King, "US, allied cyber defenders discuss interoperability at Cyber Summit 2015," online news article, Wiesbaden, Germany: 5th Signal Command Public Affairs, July 29, 2015, available from *www.army.mil/article/152994/US__allied_cyber_defenders_discuss_interoperability_at_Cyber_Summit_2015/?from=RSS,* accessed October 22, 2015.

156. "Think About It…Vigilance Begins With You," U.S. Army Europe public website, available from *www.eur.army.mil/vigilance/,* accessed October 22, 2015.

157. *Antiterrorism Awareness: The Cyber Attack Cycle*, Washington, DC: Office of the Provost Marshal General, available from *www.eur.army.mil/vigilance/Cyber_Attack_Cycle.pdf,* accessed October 22, 2015. The presentation introduction is:

> The Cyber Attack Cycle depicted in the following pages educates you on how cyber adversaries operate in order for you to better defend our networks. The 'Cyber Attack Cycle' outlines the sequential actions taken by adversaries in a cyber attack. Interrupting an adversary action anywhere along this cycle can serve to stop the attack. [These steps are:] Recon; Weaponize; Deliver; Exploit; Install; Command and Control; Action on the Objective. (p. 3)

158. Natalie Vanatta, Robert Singley, and James Torrence, "From 'Mixed Signals' European Command brings together Allies," *Army Communicator*, Vol. 40, No. 1, Spring 2015, pp. 32-37.

159. Jason Rossi, "Exercise Combined Endeavor kicks off its 20th year," U.S. European Command public website, August 14, 2014, available from *eucom.mil/media-library/article/26803/exercise-combined-endeavor-kicks-off-its-20th-year*, accessed October 21, 2015.

160. Christine June, "EUCOM J6 discusses cyber sovereignty at inaugural Marshall Center course," U.S. European Command public website, December 18, 2014, available from *eucom.mil/media-library/article/30932/eucom-j6-discusses-cyber-sovereignty-at-inaugural-marshall-center-course*, accessed October 22, 2015.

161. Shaun Cavanaugh, "Cyber Endeavor 2012 – Building Cyber Defense Capacity in our Partner Nations," U.S. European Command public website blog, February 24, 2012, available from *eucom.mil/media-library/blog%20post/23155/cyber-endeavor-2012-building-cyber-defense-capacity-in-our-partner-nations*, accessed October 22, 2015. The author includes the mission of Cyber Endeavor:

> Cyber Endeavor is the United States European Command's paramount cyber security collaboration, familiarization and engagement program designed to strengthen partner nation cyber defense capacities through seminars, events and exercise support. Cyber Endeavor builds cyber defense partnerships with NATO, partner nations, academia and industry. Its purpose is to improve force readiness for deployment in support of exercises, multinational crisis response and future missions.

162. Trina Zwicker, "Cyber Endeavor Capstone 2014 to expand on partnerships between public, private sectors," U.S. European Command public website blog, April 14, 2014, available from *eucom.mil/media-library/blog%20post/25644/cyber-endeavor-capstone-2014-to-expand-on-partnerships-between-public-private-sectors*, accessed October 22, 2015.

163. Will Poole, "First-Ever Regional Cyber Endeavor Seminar Held in Montenegro," U.S. European Command public website blog, March 13, 2012, available from *www.eucommil/media-library/blog%20post/23210/first-ever-regional-cyber-endeavor-seminar-held-in-montenegro*, accessed October 22, 2015.

164. Stephanie A. Dantzler, "Cyber Defense Partnerships Lead to Lasting Relationships," U.S. European Command public website blog, May 17, 2012, available from *www.eucom.mil/media-library/blog%20post/23386/cyber-defense-partnerships-lead-to-lasting-relationships,* accessed October 22, 2015.

165. "Poland and US join the Centre," CCD COE – News official website, Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, November 17, 2011, available from *https://ccdcoe.org/poland-and-us-join-centre.html*, accessed October 23, 2015.

166. See Multinational Capability Development Campaign, *MCDC 2013-2014 Catalog of Products*, p. 11; and Multinational Capability Development Campaign, *MCDC 2015-16 Information Paper*, p. 2.

167. Michael N. Schmitt, ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence,* Cambridge, UK: Cambridge University Press, 2013, available from *https://ccdcoe.org/tallinn-manual.html,* accessed October 23, 2015.

168. The current volume of *International Law Studies* and its searchable archive of articles is available from *stockton.usnwc.edu/ils/*, accessed October 23, 2015.

169. A dedicated Cyberlaw Edition of *The Air Force Law Review,* Vol. 64, 2009, is available from *www.afjag.af.mil/shared/media/document/AFD-091026-024.pdf,* accessed October 23, 2015.

170. *The Cyber Defense Review* is currently limited to an online-only offering that is available from *cyberdefensereview.org*, accessed October 23, 2015. The purpose of the journal is:

> The Cyber Defense Review (CDR) is positioning itself as the leading online and print journal for issues related to cyber for military, industry, professional and academic scholars, practitioners and operators interested [in] providing timely and important research to advance the body of knowledge in an inherently multi-disciplinary field. The CDR provides an unclassified venue for content divided into an online journal with longer more thoroughly researched articles and a blog with short engaging thought pieces to stir rapid discussion within the broader community. We publish original, unpublished, relevant and engaging contributed content from across the community.

171. John R. Deni, "*Fulfilling NATO's Missions: The Need for New Structures and Instruments*," Policy Brief, Transatlantic Security and Future of NATO Series, Paris, France: The George Marshall Fund of the United States-Paris, May 2015, p. 1, available from *gmfus.org/publications/fulfilling-natos-missions-need-new-structures-and-instruments*, accessed October 23, 2015.

172. *Ibid*., p. 2.

173. "Testimony of: Admiral James Stavridis, United States Navy, Commander, United States European Command before the 113th Congress, 2013," Washington, DC: Government Printing Office, March 13, 2013, p. 7, available from *armed-services.senate.gov/imo/media/doc/Stavridis%2003-19-13.pdf*, accessed October 23, 2015.

174. Philip M. Breedlove, "The New NATO," *The Three Swords: The Magazine of the Joint Warfare Centre*, No. 27, November 2014, pp. 16-19.

APPENDIX

SUMMARY OF CYBER-RELATED MATERIAL IN DECLARATIONS FROM RECENT NORTH ATLANTIC TREATY ORGANIZATION (NATO) NORTH ATLANTIC COUNCIL MEETINGS

NATO North Atlantic Council Meeting	Key Cyberspace-Related Text in Summit Declaration
Prague, Czech Republic November 21, 2002	4. Effective military forces, an essential part of our overall political strategy, are vital to safeguard the freedom and security of our populations and to contribute to peace and security in the Euro-Atlantic region. We have therefore decided to: f. Strengthen our capabilities to defend against cyber attacks.[1]
Istanbul, Turkey June 28, 2004	No mention of cyber in declaration.
Brussels, Belgium February 25, 2005	No mention of cyber in declaration.
Riga, Latvia November 29, 2006	The adaptation of our forces must continue. We have endorsed a set of initiatives to increase the capacity of our forces to address contemporary threats and challenges. These include: • work to develop a NATO Network Enabled Capability to share information, data and intelligence reliably, securely and without delay in Alliance operations, while improving protection of our key information systems against cyber attack[2]
Bucharest, Hungary April 3, 2008	47. NATO remains committed to strengthening key Alliance information systems against cyber attacks. We have recently adopted a Policy on Cyber Defence, and are developing the structures and authorities to carry it out. Our Policy on Cyber Defence emphasises the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack. We look forward to continuing the development of NATO's cyber defence capabilities and strengthening the linkages between NATO and national authorities.[3]

NATO North Atlantic Council Meeting	Key Cyberspace-Related Text in Summit Declaration
Strasbourg-Kehl, France/Germany April 2-3, 2009	49. We remain committed to strengthening communication and information systems that are of critical importance to the Alliance against cyber attacks, as state and non-state actors may try to exploit the Alliance's and Allies' growing reliance on these systems. To prevent and respond to such attacks, in line with our agreed Policy on Cyber Defence, we have established a NATO Cyber Defence Management Authority, improved the existing Computer Incident Response Capability, and activated the Cooperative Cyber Defence Centre of Excellence in Estonia. We will accelerate our cyber defence capabilities in order to achieve full readiness. Cyber defence is being made an integral part of NATO exercises. We are further strengthening the linkages between NATO and Partner countries on protection against cyber attacks. In this vein, we have developed a framework for cooperation on cyber defence between NATO and Partner countries, and acknowledge the need to cooperate with international organisations, as appropriate.[4]
Lisbon, Portugal November 20, 2010	40. Cyber threats are rapidly increasing and evolving in sophistication. In order to ensure NATO's permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO's doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber attack against systems of critical importance to the Alliance. We will strive in particular to accelerate NATO Computer Incident Response Capability (NCIRC) to Full Operational Capability (FOC) by 2012 and the bringing of all NATO bodies under centralised cyber protection. We will use NATO's defence planning processes in order to promote the development of Allies' cyber defence capabilities, to assist individual Allies upon request, and to optimise information sharing, collaboration and interoperability. To address the security risks emanating from cyberspace, we will work closely with other actors, such as the UN and the EU, as agreed. We have tasked the Council to develop, drawing notably on existing international structures and on the basis of a review of our current policy, a NATO in-depth cyber defence policy by June 2011 and to prepare an action plan for its implementation.[5]

NATO North Atlantic Council Meeting	Key Cyberspace-Related Text in Summit Declaration
Chicago, Illinois, USA May 20, 2012	49. Cyber attacks continue to increase significantly in number and evolve in sophistication and complexity. We reaffirm the cyber defence commitments made at the Lisbon Summit. Following Lisbon, last year we adopted a Cyber Defence Concept, Policy, and Action Plan, which [is] now being implemented. Building on NATO's existing capabilities, the critical elements of the NATO Computer Incident Response Capability (NCIRC) Full Operational Capability (FOC), including protection of most sites and users, will be in place by the end of 2012. We have committed to provide the resources and complete the necessary reforms to bring all NATO bodies under centralised cyber protection, to ensure that enhanced cyber defence capabilities protect our collective investment in NATO. We will further integrate cyber defence measures into Alliance structures and procedures and, as individual nations, we remain committed to identifying and delivering national cyber defence capabilities that strengthen Alliance collaboration and interoperability, including through NATO defence planning processes. We will develop further our ability to prevent, detect, defend against, and recover from cyber attacks. To address the cyber security threats and to improve our common security, we are committed to engage with relevant partner nations on a case-by-case basis and with international organisations, inter alia the EU, as agreed, the Council of Europe, the UN and the OSCE, in order to increase concrete cooperation. We will also take full advantage of the expertise offered by the Cooperative Cyber Defence Centre of Excellence in Estonia.[6]

NATO North Atlantic Council Meeting	Key Cyberspace-Related Text in Summit Declaration
Newport, Wales, UK September 5, 2014	72. As the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, we have endorsed an Enhanced Cyber Defence Policy, contributing to the fulfillment of the Alliance's core tasks. The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. It recalls that the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks. Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis. 73. We are committed to developing further our national cyber defence capabilities, and we will enhance the cyber security of national networks upon which NATO depends for its core tasks, in order to help make the Alliance resilient and fully protected. Close bilateral and multinational cooperation plays a key role in enhancing the cyber defence capabilities of the Alliance. We will continue to integrate cyber defence into NATO operations and operational and contingency planning, and enhance information sharing and situational awareness among Allies. Strong partnerships play a key role in addressing cyber threats and risks. We will therefore continue to engage actively on cyber issues with relevant partner nations on a case-by-case basis and with other international organisations, including the EU, as agreed, and will intensify our cooperation with industry through a NATO Industry Cyber Partnership. Technological innovations and expertise from the private sector are crucial to enable NATO and Allies to achieve the Enhanced Cyber Defence Policy's objectives. We will improve the level of NATO's cyber defence education, training, and exercise activities. We will develop the NATO cyber range capability, building, as a first step, on the Estonian cyber range capability, while taking into consideration the capabilities and requirements of the NATO CIS School and other NATO training and education bodies.[7]

ENDNOTES - APPENDIX

1. "Prague Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague on 21 November 2002," NATO Press Release (2002)133, North Atlantic Treaty Organization, November 21, 2002, available from *nato.int/docu/pr/2002/p02-127e.htm,* accessed September 8, 2015.

2. "Riga Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006," NATO Press Release (2006)150, North Atlantic Treaty Organization, November 29, 2006, available from *nato.int/cps/en/natolive/official_texts_37920.htm,* accessed August 25, 2015.

3. "Bucharest Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008," NATO Press Release (2008)049, North Atlantic Treaty Organization, April 3, 2008, available from from *nato.int/cps/en/natolive/official_texts_8443.htm*, accessed August 25, 2015.

4. "Strasbourg/Kehl Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg," NATO Press Release (2009)044, North Atlantic Treaty Organization, April 4, 2009, available from *nato.int/cps/en/natolive/news_52837.htm,* accessed March 25, 2016.

5. "Lisbon Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon," NATO Press Release (2010)155, North Atlantic Treaty Organization, November 20, 2010, available from *nato.int/nato_static_fl2014/assets/pdf/pdf_2010_11/2010_11_11DE1DB9B73C4F9BBFB52B2C94722EAC_PR_CP_2010_0155_ENG-Summit_LISBON.pdf,* accessed August 25, 2015.

6. "Chicago Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012," NATO Press Release (2012)062, North Atlantic Treaty Organization, May 20, 2012,

available from nato.int/cps/en/natolive/off*icial_texts_87593.htm?mode=pressrelease, accessed August 25, 2015.*

7. "Wales Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales," Press Release (2014)120, North Atlantic Treaty Organization, September 5, 2014, available from *nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease,* accessed August 25, 2015.

U.S. ARMY WAR COLLEGE

Major General William E. Rapp
Commandant

*****

STRATEGIC STUDIES INSTITUTE
and
U.S. ARMY WAR COLLEGE PRESS

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven K. Metz

Author
Mr. Jeffrey L. Caton

Editor for Production
Dr. James G. Pierce

Publications Assistant
Ms. Denise J. Kersting

*****

Composition
Mrs. Jennifer E. Nevil

U.S.ARMY

THE
UNITED STATES
ARMY WAR COLLEGE

STRENGTH and WISDOM

FOR THIS AND OTHER PUBLICATIONS, VISIT US AT
http://www.carlisle.army.mil/

ISBN 1-58487-728-6
9 781584 877288
90000>

This Publication

SSI Website

USAWC Website